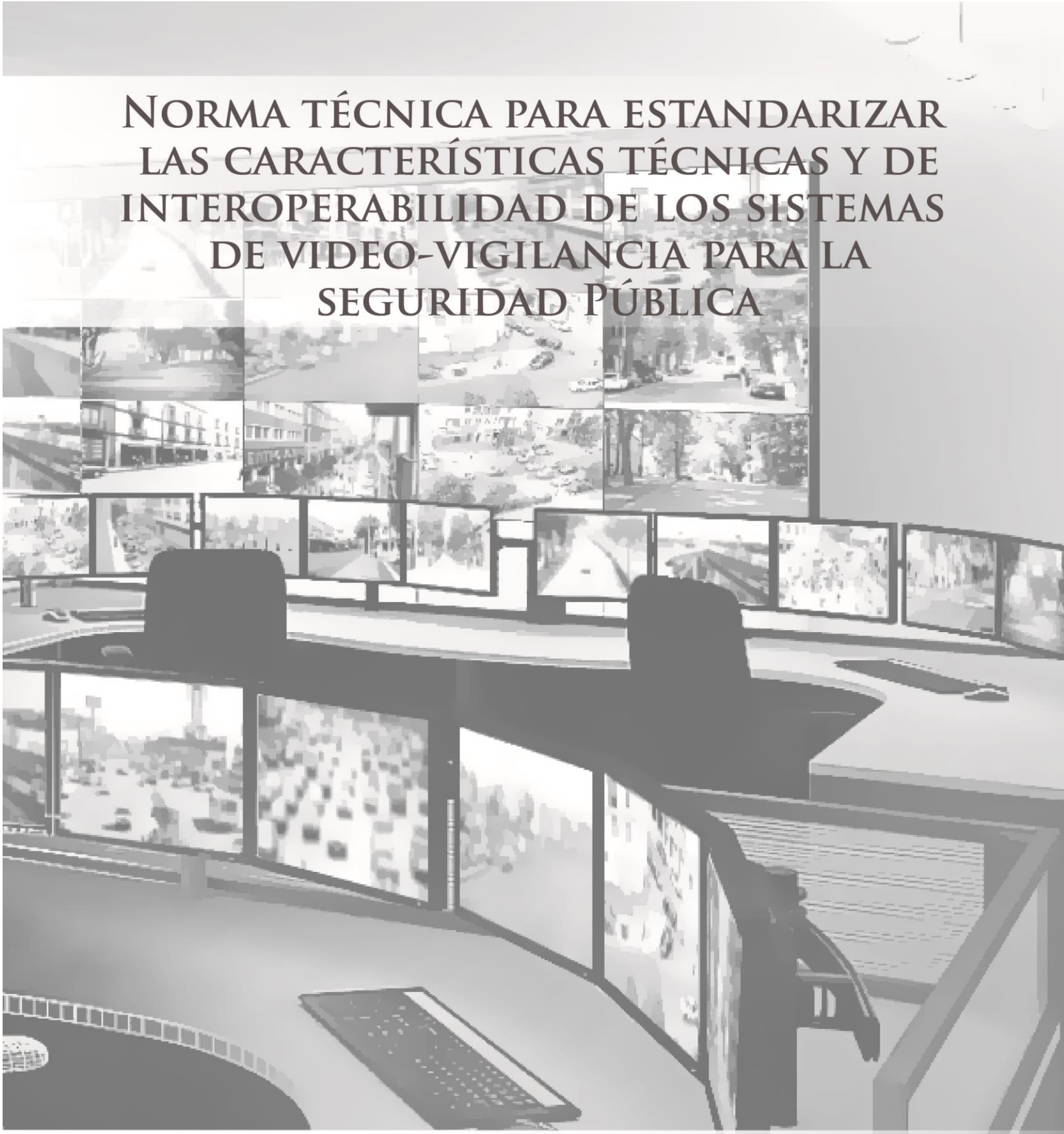
Norma técnica para estandarizar las características técnicas y de interoperabilidad de los sistemas de video-vigilancia para la seguridad Pública



SEGOB
SECRETARÍA DE GOBERNACIÓN

ESTADOS UNIDOS MEXICANOS

CENTRO NACIONAL DE INFORMACIÓN

SECRETARIADO EJECUTIVO
DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA

SISTEMA NACIONAL DE SEGURIDAD PÚBLICA

Contenido

I. PRESENTACIÓN.

Un Sistema de Video Vigilancia (SVV) puede definirse como una herramienta tecnológica que, a través de cámaras de video localizadas estratégicamente e interconectadas entre sí, permiten apoyar la operación y despliegue policial, la atención de emergencias, la prevención del delito y la procuración de justicia.

Desde hace tiempo, México ha incursionado, a través de sus organizaciones y cuerpos de seguridad, con sumo interés en las aplicaciones de la video vigilancia como mecanismo para proporcionar mayor seguridad a la sociedad, principalmente en ambientes urbanos.

En la actualidad, los SVV se han constituido como valiosas herramientas para la asistencia de los cuerpos de seguridad, cuyo alcance y eficiencia dependen, en buena parte, de una apropiada selección de la tecnología. La adecuada implementación de los SVV mejora la seguridad de la ciudadanía mediante el monitoreo de ambientes abiertos y cerrados, tales como calles y avenidas, bancos, supermercados, áreas de estacionamiento, edificios, entre otros. Esto permite ampliar la capacidad de reacción de las fuerzas del orden en casos que amenazan la integridad de las personas, como accidentes, incendios u otro tipo de eventualidades.

Por ello es importante que la implementación de equipos y sistemas en México se realice a partir de un instrumento técnico normativo que establezca las características óptimas de los SVV en sus distintos componentes, así como métricas y herramientas para su evaluación y gestión.

En este sentido, el Sistema Nacional de Seguridad Pública (SNSP), en su Trigésimo Novena Sesión Ordinaria del Consejo Nacional de Información celebrada el 18 de diciembre de 2015, instruyó al Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) a elaborar una Norma Técnica para estandarizar las características técnicas y de interoperabilidad de los Sistemas de Video Vigilancia para la Seguridad Pública.

El Secretariado Ejecutivo, por conducto del Centro Nacional de Información (CNI), y con el apoyo experto del Instituto Politécnico Nacional, elaboró el estándar técnico, mismo que fue puesto a consideración y aprobado por el Consejo Nacional de Seguridad Pública, en su XL Sesión celebrada el 30 de agosto de 2016.

Este documento presenta la norma resultado de dichos trabajos, fundamentado en el estudio normativo y aplicativo de los SVV, tanto nacional como internacionalmente, y considerando las características de varios de sistemas ya instalados en el México.

El documento se divide en los siguientes apartados: I) la **presentación**, que incluye la estructura general y una descripción de los seis capítulos que componen a la investigación; II) la definición del **objetivo** de la norma; III) la **fundamentación**, que explica con mayor detalle qué es un SVV y qué elementos lo componen; los parámetros de densidades, alturas y localización georreferenciada; y el procedimiento de desarrollo; y IV) la **Norma**, dividida en capítulos que corresponden a los parámetros a cumplir por parte de los nuevos diseños de SVV.

Cada uno de los elementos de la Norma tiene un fundamento teórico, práctico y normativo. Estos elementos se presentarán en un **Anexo Técnico**, a publicarse como complemento de apoyo para la Norma.

Finalmente, se debe considerar que el presente documento habrá de mantenerse en revisión y mejora continua, a fin de asegurar su vigencia y operatividad, en conjunto con las instancias competentes del Sistema Nacional de Seguridad Pública.

II. OBJETIVO.

La presente Norma establece los criterios normativos y técnicos que dicten a las entidades federativas las características técnicas y la forma de operación de los Sistemas de Video Vigilancia (SVV). En esta Norma se establecen los parámetros para la organización, infraestructura, tecnología y evaluación de los SVV de conformidad con la Ley General del Sistema Nacional de Seguridad Pública, que considera la participación directa de los tres órdenes de gobierno, con base en los siguientes rubros:

II.1. Infraestructura: Se proporcionan estándares con mínimos indispensables, obtenidos del estudio minucioso de las tecnologías de última generación y de los sistemas actualmente instalados en México, así como de la experiencia en campo de los creadores de esta norma. Esta consideración permitirá desarrollar adecuadamente las instalaciones estratégicas de los SVV.

II.2. Coordinación: Se definen los sistemas e infraestructuras tecnológicas de última generación que deben estar presentes en los SVV para la mejor coordinación con las corporaciones e instancias responsables de la seguridad ciudadana.

II.3. Organización: Se establecen las condiciones de organización operativa que deben estar presentes en los SVV para su mejor operación y coordinación con las corporaciones instancias responsables de la seguridad ciudadana.

II.4. Operación: Se establecen los requisitos que soporten la documentación del sistema de gestión y operación de un SVV.

II.5. Evaluación: Se determinan los indicadores a los que se deberán apegar los SVV para medir el cumplimiento de los estándares presentes en esta Norma.

III. FUNDAMENTO.

III.1 Fundamento sociopolítico.

Como se describe anteriormente, un Sistema de Video Vigilancia (SVV) puede definirse como una herramienta tecnológica que, a través de cámaras de video localizadas estratégicamente e interconectadas entre sí, permiten apoyar la operación y despliegue policial, la atención de emergencias, la prevención del delito y la procuración de justicia.

Para la seguridad pública, los SVV presentan diversas ventajas. En primer lugar, la video vigilancia incrementa la capacidad de operación, puesto que incrementa la capacidad de visión a prácticamente 24 horas por 365 días. Sus efectos pueden catalogarse en dos dimensiones principales: como un disuasor de delitos y como coadyuvante en la investigación policiaca.

La instalación de SVV se rige bajo el principio de que si el delincuente percibe mayor certeza de ser capturado, disminuirán las posibilidades de involucrarse en alguna actividad criminal. Es decir, la video vigilancia puede funcionar de manera positiva para reducir el riesgo de ser víctima de un delito, a la vez de que permite que las autoridades cuenten con material que sirva como evidencia para una denuncia futura. Derivado de la reducción de la criminalidad, un incremento en la sensación de seguridad puede acarrear impactos benéficos para la cohesión social en una comunidad, e incluso, en una ciudad o un estado.

Los SVV monitorean a multitudes y a individuos, responden a posibles amenazas y alertan a los operadores sobre comportamientos y acciones de riesgo antes, durante y después de que ocurra un evento. Así mismo, su uso se extiende más allá del mantenimiento del orden público, ayudando a informar y dirigir tareas en situaciones como incendios y/o desastres naturales.

A diferencia de otros mecanismos, los SVV representan una alternativa con un mejor balance entre costo y beneficio en el manejo de la seguridad pública. La video vigilancia es una mejor inversión que el personal de seguridad en términos de eficiencia.

A diferencia del recurso humano patrullando las calles, un SVV no es susceptible de fatiga o pérdida de concentración, lo que implica un esfuerzo ininterrumpido, constante y consistente. A pesar de que el gasto hecho en un SVV podría parecer mayor, en el largo plazo representa una forma de ahorra en comparación con la contratación de oficiales de policía adicionales.

La video vigilancia parece tener un efecto positivo no solamente en la disuasión del delito, sino también en las propias tareas de los elementos de policía en tierra. Cuando la video vigilancia opera en coordinación con los organismos de mantenimiento del orden, la policía percibe una mayor certidumbre en el desempeño de su labor. Así, la inversión no sustituye a las capacidades del elemento humano, sino que extiende sus posibilidades y le brinda mayor seguridad para la realización de su trabajo.

Esta cuestión remarca la necesidad de la Norma de proponer una interoperabilidad no solo en un carácter técnico, sino también que busque la cooperación y la coordinación entre los agentes del orden, y la complementariedad de la video vigilancia con otras medidas de reducción del crimen (el patrullaje policial, el alumbrado público, los programas de prevención, por mencionar algunos).

III.2 Fundamento jurídico.

A pesar de las ventajas que se han enumerado anteriormente, los SSV representan un debate continuo con la sociedad civil sobre el balance que debe existir entre la seguridad pública y derechos como la privacidad, la trasparencia o la proporcionalidad. La Comisión Europea para la Democracia a través de la Ley (2007) explica que, en el espacio público, las personas tienen una expectativa menor de privacidad, aunque eso no implica que esperen ser privados de sus libertades y derechos en su esfera privada.

Al respecto, la *Carta para el uso democrático de la vigilancia por video*[1], elaborada por el Foro Europeo de Seguridad Urbana (2013), establece varios puntos en común con los

[1] http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_ES.pdf

objetivos de esta Norma, tales como a) la realización de diagnósticos previos para definir objetivamente las necesidades locales; b) la implementación de evaluaciones periódicas; c) la formación de los operadores de los sistemas de video vigilancia; y d) una autoridad de control que verifique los principios enunciados. Todos estos puntos son abordados de manera puntual por la presente Norma.

Estos lineamientos deberán considerar el respeto irrestricto a los derechos humanos, que deberán ser observados durante todo el proceso de planeación, diseño, implementación y operación del SSV. El seguimiento de los principios de equilibrio democrático, racionalidad, evaluación, proporcionalidad, integralidad y transparencia es indispensable en una estrategia de seguridad pública eficiente, congruente con el estado de derecho, y acorde con los estándares jurídicos nacionales e internacionales en la materia.

La creación de esta Norma obedece a la necesidad de un ordenamiento que no solo garantice un mejor uso de los recursos públicos para seguridad, sino que también permita establecer criterios en la planeación, diseño, implementación y operación de los SVV con base en la necesidad, proporcionalidad e integralidad de las medidas de prevención y contención del delito. Esta medida coadyuva a contemplar una visión multifactorial de la problemática a resolver.

Este documento sugiere la observancia de los derechos a la privacidad y la no discriminación, de modo que las tecnologías de grabación de audio, reconocimiento facial y reconocimiento biométrico, se hagan uso con apego a la ley. De igual manera, capacitar al personal que opere los SVV a evitar tomen decisiones bajo prejuicios de raza, género, origen, idioma, posición económica, entre otros; ni que el uso de las cámaras de seguridad pública sea efectuado al interior de domicilios y espacios privados.

El uso de los SVV es compatible con el Estado de Derecho y los principios de la sociedad democrática en tanto existan mecanismos que regulen su uso y aplicación dentro de los estándares de la legalidad. Esta Norma es el primer paso para lograr esta meta.

III.3 Fundamento técnico.

En general, el SVV se compone de la asociación precisa entre tres elementos: 1) cámaras, 2) comunicaciones y 3) centro de monitoreo. La captura de imágenes es, en realidad, solo el principio del proceso. Las cámaras están conectadas con los centros de monitoreo a través de un sistema de comunicaciones, el cual debe diseñarse *ad hoc* para cada sitio donde se instala el SVV. Es en el centro de monitoreo donde se toman las decisiones en tiempo real por uno o varios cuerpos de seguridad o de atención a la ciudadanía. La Figura III.1 es una visión general que muestra los elementos que conforman el sistema, que se abordan a detalle de forma transversal en los siguientes capítulos.

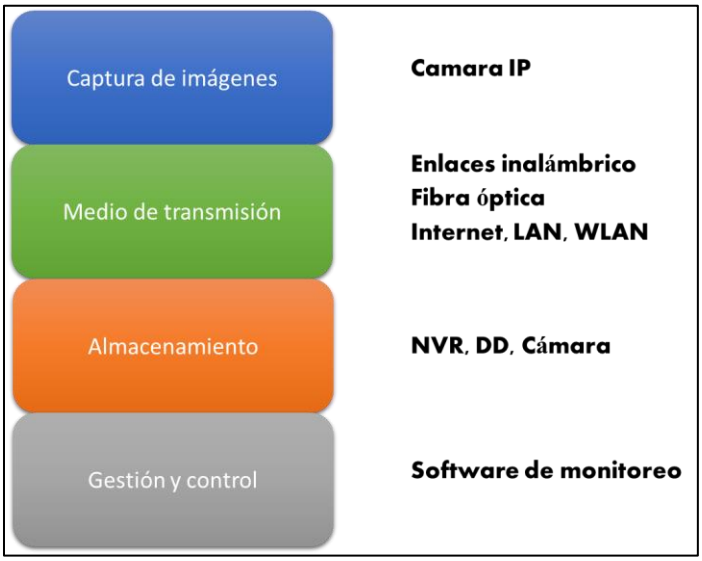


Figura III.1 Esquema General de un SVV[2]

En la Figura III.1 se resumen los componentes básicos que integran un Sistema de Video-Vigilancia (SVV): La captura de imágenes por medio de cámaras, transmisión de datos (imagen, audio, video) por medio de red alámbrica o inalámbrica, almacenamiento de datos y, por último, la gestión de video.

[2] Tesis: “Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia”.

El esquema contempla los elementos comúnmente usados en los sistemas actuales en México. Un SVV contiene el Punto de Monitoreo Inteligente (PMI) con diferentes dispositivos, además de las cámaras, que son descritos en el capítulo correspondiente.

La información recogida en el poste es llevada al Centro de Control a través del sistema de comunicaciones, que puede usar diferentes tecnologías para cumplir con su función. Finalmente la información de los PMI se recibe en los Centros de Control, donde la información es procesada y transferida a otras entidades que las usan.

Aunque no aparecen en el esquema, dos temas más son tratados en este documento: por un lado, las características de los postes que se usarán en los PMI, las cuales son diferentes en altura y constitución, porque dependen primero de lo que se quiere “ver” y de la profundidad de la visión, así como de las características del suelo y principalmente las condiciones climáticas y de velocidad del viento. La altura y constitución no son temas menores puesto que no solo inciden en la perspectiva de la cámara, sino también en la visibilidad que los ciudadanos (y aquellas personas que planeen actos delictivos, principalmente) tienen de estas.

Por otro lado, un SVV dedicado a la seguridad debe definir tanto el número como la posición de las cámaras, en función de temas como índice poblacional, estructura urbana, y sobre todo los lugares donde se cometen delitos. El proceso de planeación para determinar las características, requerimientos y alcances de los SVV los hace esencialmente diferentes, sin embargo, los esquemas que se proponen en este documento podrán adaptarse a la mayoría de los planteamientos técnicos y de logística de cada caso.

El diseño del SVV sigue un proceso lógico que se describe a continuación en forma breve usando el diagrama de la Figura III.2, que establece las fases y la secuencia de ejecución. Aunque se denotan fases continuas, en cualquier momento puede regresarse en el tiempo para realizar ajustes originados por cambios en el entorno, la tecnología, los requerimientos o las limitantes de presupuesto.

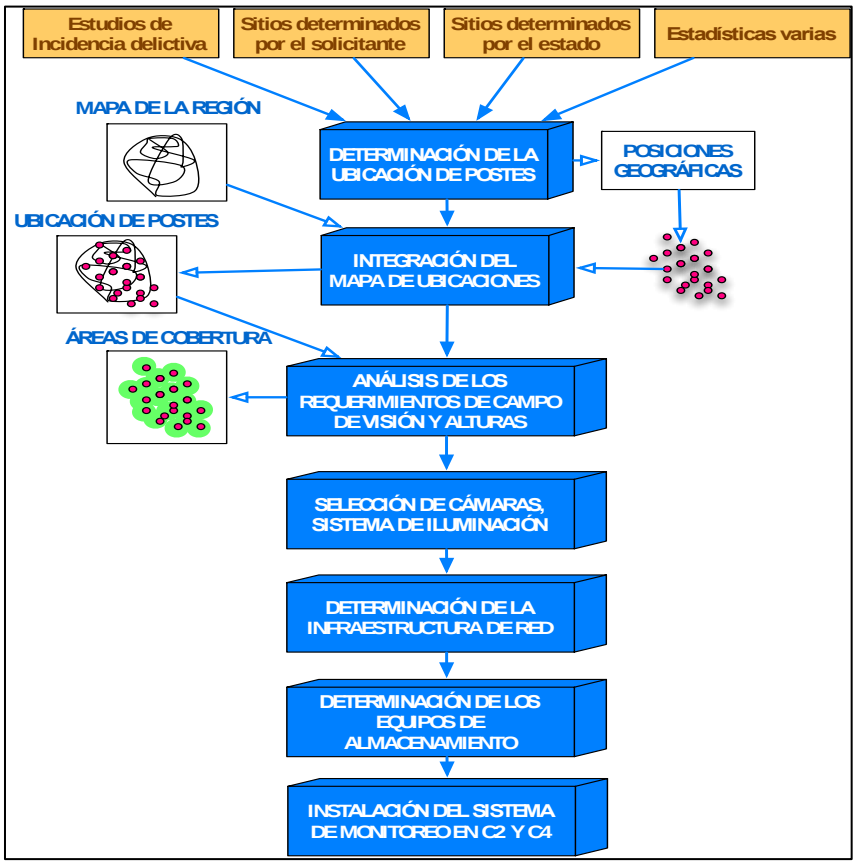


Figura III.2 Procedimiento para la implantación de un SVV

El proceso del diseño del sistema inicia con la determinación de la ubicación de los postes del SVV. Esta es la primera fase del proceso y recibe información de diversas fuentes, tales como datos de incidencia delictiva, los sitios determinados por el solicitante, los sitios determinados por el Estado y el resultado de diversas estadísticas nacionales y locales. Todas estas fuentes justifican la posible instalación de un nodo en el SVV. Sin embargo es necesario ordenar por prioridad cada requerimiento de instalación de un poste (con cámaras), por lo que se requiere analizar y cruzar toda la información disponible para la región en estudio.

Una vez definidas las prioridades, se establece la lista de posiciones georreferenciadas donde se propone la ubicación de cada PMI. Mediante un software de Información Geográfica (SGI), se integran las posiciones propuestas en un mapa temático de la región, que incluye todos los aspectos relevantes para la instalación de la infraestructura:

edificios, calles, carreteras, instalaciones, postes, árboles, ductos, comercios, escuelas, así como índices delictivos georreferenciados y cualquier otro requerimiento que el diseñador decida. Cada uno de ellos se toma en cuenta para la decisión de instalación de los PMI. Como complemento se puede tener una lista de posiciones georreferenciadas con la propuesta de la ubicación de cada poste (cámaras).

Las posiciones propuestas para los PMI en el mapa temático con las capas georreferenciadas necesarias son el punto de partida para definir los requerimientos de campo de visión y altura de los postes. Se procede a realizar el estudio en campo para determinar los campos de visión, tanto en profundidad como en extensión; y las alturas de los postes donde se ubicarán las cámaras, creando el entorno real de instalación del SVV.

Posteriormente, se determina el número de cámaras a instalar, los tipos, las orientaciones, resoluciones, tipos de lentes, sistemas de iluminación y todos los aspectos relevantes que permitan ajustar el sistema a las características de la región. Este es la fase más demandante en tiempo, y es la clave para alcanzar los objetivos planteados como parte del SVV.

A partir de las posiciones definidas en el mapa temático, es posible realizar el estudio que culmina con el diseño de la infraestructura de comunicaciones necesaria para dar soporte a la transmisión de video y señalización dentro del SVV. La determinación del tipo de redes y medios se basa en la infraestructura instalada en la región, los requerimientos en base al tipo de cámaras propuestas y los datos de escalabilidad del proyecto.

Por otro lado, las características de la infraestructura de la red permiten definir la posición y la cantidad necesaria de los Centros de Control secundarios. La localización de estos también pueden definirse en función de las posibilidades logísticas y la necesidad del sistema de seguridad para contar con ellos en posiciones estratégicas.

Las características definidas hasta este momento guían la selección del equipo y capacidades de almacenamiento. Los equipos de post-procesamiento dependen, en gran medida, de los procesos de análisis definidos como parte de la integración general del SVV.

Por su parte, el sistema de monitoreo se refiere al número de pantallas que pueden ser visualizadas por un operador, tanto en cantidad como en tiempo, considerando que es posible cambiar periódicamente las cámaras visibles en la pantalla. El número de monitores está relacionado con las dimensiones del sistema y la cantidad visible de PMI en cada uno, de acuerdo a las posibilidades analíticas de los operadores, en relación con su capacidad de concentración y discriminación para definir un evento importante en el total de cámaras captadas en un monitor.

Como se puede observar en el documento, las decisiones técnicas para la implementación del SVV pasan van más allá de los requerimientos tecnológicos para incluir elementos de naturaleza distinta, tales como los sociopolíticos (la selección de los puntos de instalación con base en la incidencia delictiva, por ejemplo) y otros de índole jurídica (como la capacitación de los operadores para el uso del sistema dentro del marco de la legalidad. La dimensión técnica debe tomar en cuenta a las otras partes, de modo que la estrategia del SVV sea integral e interoperable.

III.4 Fundamento metodológico.

En cada uno de los apartados que componen la Norma Técnica se describen las referencias normativas, así como los fundamentos teóricos y prácticos que han llevado a la definición de características mínimas aplicables para cada elemento que conforma el SVV. Los elementos mínimos plenamente justificados por la teoría y la práctica representan la **NORMA,** es decir, las reglas específicas a las que habrán de sujetarse los solicitantes de apoyo para la construcción de sistemas nuevos.

Localización. Describe la forma en que deben tomarse las decisiones respecto de la localización de los postes tecnológicos, basadas en la descripción de los diferentes centros urbanos existentes en el país en función del número de habitantes, pero también considerando los índices delictivos, los cuales permiten establecer con precisión zonas de alto riesgo en donde las cámaras de video vigilancia deberán cumplir con una función preventiva y de reacción.

Diseño de Postes y Cimentaciones. Se refiere a un detallado estudio relacionado con las características climáticas y de suelo de toda la República Mexicana que permiten definir las características mecánicas de los postes y de su cimentación, se presenta en este capítulo tablas y mapas que deberán ser considerados por cada entidad con el fin de que un sistema de alta seguridad, como el que nos ocupa, tenga posibilidades de mantenerse activo, con mantenimiento preventivo adecuado, durante varios años; el tiempo de vida de los postes habrá que establecerlo tanto en función de la durabilidad de sus materiales como en el costo de su construcción.

Punto de Monitoreo Inteligente. Este capítulo se refiere a las características del equipo que se monta sobre los postes y que se refieren en el documento como Puntos de Monitoreo Inteligente (PMI). Aunque además de las cámaras, algunos sistemas instalan otro tipo de equipo como botones de pánico, bocinas de alerta e incluso detectores de disparo, y que en esta parte se describen en función de sus características técnicas, el capítulo pone mayor énfasis en las cámaras de Video Vigilancia, no solamente definiendo

sus características, sino también estableciendo métodos para calcular la profundidad de visión así como el área de cobertura en función de los lentes que usen.

Telecomunicaciones. El sistema de comunicaciones del SVV es el tema de este capítulo, se considera una multiplicidad de enlace entre los PMI y los centros de control, que van desde los inalámbricos de microondas, hasta los de fibra óptica. Se analiza igualmente la estructura de diferentes sistemas, desde los simples con un enlace único de microondas hasta los de múltiples enlaces e híbridos que emplean igualmente fibra óptica. Para cada forma de comunicaciones se establecen protocolos de comunicaciones, basados en normas y recomendaciones técnicas, así como la descripción de cada uno de los elementos que conforman el sistema.

Centro de Control. En este capítulo se abordan las características técnicas de todos los elementos que existen en el Centro de Control, desde la red LAN dentro del edificio, hasta los equipos de distribución de información, de monitoreo, de almacenamiento y las necesarias fuentes de energía eléctrica, que deben mantener el funcionamiento del sistema aún con fallas de la red eléctrica pública.

Operación. Incluye la descripción de operación del SVV así como una organización administrativa mínima que haga eficientes sus procesos internos. Igualmente se describen elementos mínimos que deben cumplir los Recursos Humanos que trabajen en los Centros de Operación.

IV. NORMA.

De acuerdo a los principios fundamentales de esta norma, se ha realizado este documento que concentra el resultado de fuentes como el estudio y sistematización de los reportes generados durante las visitas de campo; el análisis de los estándares nacionales e internacionales; y la consulta de la normas y de artículos científicos aplicables a los SVV. Los requerimientos mínimos que deberán cumplir los sistemas de video vigilancia se establecen en seis apartados:

- **Localización**
- **Postes**
- **Punto de monitoreo inteligente**
- **Telecomunicaciones**
- **Centro de control**
- **Operación**

Cada apartado se integra de una **justificación**, donde se expone la importancia de la característica abordada; un **glosario**, que permite entender los términos clave de la Norma; y el desarrollo de los **lineamientos** para la implementación de cada parte. Es de gran importancia resaltar que, para consultar a profundidad cada uno de los temas presentados, será indispensable acudir al apartado de **Anexo Técnico**.

IV.1 Localización.

IV.1.1 Justificación.

La ubicación de los sistemas de video vigilancia es clave para el adecuado funcionamiento de la estrategia de seguridad pública. Los SSV son una herramienta versátil, que puede fortalecer la capacidad de las autoridades para mantener un control urbano capaz de adaptarse a diversos contextos y situaciones donde la configuración espacial se convierte en un factor sustancial para determinar sus alcances.

En buena medida, el éxito de un SVV para la seguridad pública depende del conocimiento que se tiene sobre el espacio donde se utiliza. Por tanto, este apartado considera las variables para el diseño e implementación de los nodos de un SVV con base en los parámetros de densidad y localización, considerando factores como el tamaño de las ciudades o municipios, su densidad poblacional, la concentración de unidades económicas, la concentración de delitos, entre otros. Así mismo, se recogen los principales indicadores para la realización del análisis recomendado y, en consecuencia, de una mejor planeación financiera.

IV.1.2 Glosario.

- Cobertura: El área que alcanza a cubrir una cámara de vídeo vigilancia visualmente; también puede ser llamado campo de acción.
- Densidad: Número de cámaras de vídeo vigilancia que se sugiere instalar en función de cada unidad de área.
- Derecho a la no discriminación: Para efectos de este trabajo, se considera como una garantía de protección otorgada a la no implementación de estrategias de vídeo vigilancia basadas en cuestiones de raza, género, religión, origen, idioma, posición económica o cualquier otra de origen nacional o social.

- Derecho al libre tránsito: Para efectos de este trabajo, se considera como una garantía de protección otorgada al uso irrestricto de los espacios públicos y espacios privados de uso público, en virtud de los lineamientos estipulados por la legislación vigente.
- Derecho a la privacidad: Garantía de protección otorgada a los aspectos de la vida personal de un individuo, sea que se desarrollen en un entorno reservado o público.
- Derecho a la protección de datos personales: Garantía de protección otorgada a la información que se genera de manera directa o indirecta, durante el desarrollo de la vida cotidiana de los individuos.
- Desplazamiento delictivo: Fenómeno que resulta de la implementación de estrategias de prevención del delito en una zona. Consiste en la redistribución de las conductas delictivas en términos funcionales (tipo de delito), temporales (horarios o días), tácticos (modus operandi), geográficos (zona de operación) o de objetivo.
- Doctrina de la seguridad: Indica los antecedentes teóricos y conceptuales que dan forma a las políticas y estrategias de combate al fenómeno delictivo.
- Espacio privado de acceso público: Toda infraestructura provista y administrada directamente por entidades privadas, que por su estructura y actividad desarrollada, permiten el acceso limitado o restringido de personas a sus instalaciones.
- Espacio público: Integra toda la infraestructura provista y administrada directamente por el Estado y que en función de lo especificado por la legislación vigente, puede ser utilizada por la población en general.
- Gobernabilidad: Ejercicio del poder político caracterizado por enfatizar prácticas de coparticipación entre las instituciones gubernamentales y actores no estatales, para fortalecer la toma de decisiones para el desarrollo de políticas públicas.
- Gobernanza: Conjunto de normas y reglas que regulan el marco de actuación de los procesos de coparticipación entre el estado y los actores no gubernamentales.

- Hot Spot: Técnica de análisis espacial que permite visualizar gráficamente el espacio donde se concentra una mayor densidad de delitos.
- Incidencia Delictiva: Se refiere al número de eventos delictivos en un lugar y periodo determinado. Para efectos de este documento, se adopta la definición utilizada por el SESNSP, que la entiende como el número total de delitos reportados por las instituciones de procuración de justicia.
- Indicadores: Conjunto de variables socioeconómicas, urbanas y de incidencia delictiva utilizadas para la generación de un modelo de seguridad pública multifactorial, medible y representable en el territorio, para la emisión de recomendaciones normativas respecto de la localización y densidad de los dispositivos de vídeo vigilancia.
- Localización: Sección del territorio donde se sugiere instalar las plataformas tecnológicas de vídeo vigilancia, en función de indicadores socioeconómicos, urbanos y de incidencia delictiva.
- Prevención del delito: Conjunto de medidas para la creación de una política pública destinada a inhibir o reducir la incidencia delictiva en un lugar y periodo determinado. En función de sus pautas de acción, puede entenderse como prevención situacional o prevención social del delito.
- Prevención situacional del delito: Modelo teórico-conceptual que permite la gestión del fenómeno delictivo. Parte de una perspectiva racional y económica de la actividad delincuencial, para generar estrategias que reduzcan las oportunidades de llevar a cabo un ilícito, mediante el aumento del riesgo, real o percibido, de ser detenido y la reducción al mínimo de los beneficios potenciales del acto delictivo.
- Prevención social del delito: Modelo teórico-conceptual que permite la gestión del fenómeno delictivo. Parte de una perspectiva etiológica de la actividad delincuencial, para modificar condiciones estructurales que mejoren la calidad de vida de la población en el ámbito biológico, psicológico y de desarrollo social.
- Productos de inteligencia: Instrumentos y herramientas de aplicación práctica que refuerzan la operación de las instituciones de seguridad pública; son el resultado

de la sistematización y análisis de la información cuantitativa y cualitativa recabada por el SVV.

- Seguridad nacional: En congruencia con el marco jurídico vigente, es el conjunto de estrategias de inteligencia y contrainteligencia utilizadas para prevenir, disuadir, contener o neutralizar riesgos y amenazas contra la integridad, estabilidad y permanencia del Estado mexicano.
- Seguridad pública: De acuerdo al marco jurídico mexicano, es una función a cargo del Estado, que tiene como fines salvaguardar la integridad y derechos de las personas, así como preservar las libertades, el orden y la paz públicos.

IV.1.3 Lineamientos para la elaboración de estudios de localización y densidad para instalación de Punto de Monitoreo Inteligente (PMI).

Para garantizar la efectividad de un SVV que desempeñe labores de seguridad pública, es importante partir de la aplicación de estándares técnico-científicos para determinar la mejor localización y densidad de los Puntos de Monitoreo Inteligente (PMI). Esta sección está dedicada al desarrollo de una metodología para ejecutar estudios de localización y densidad, respaldados por un modelo teórico-jurídico de prevención situacional[3] y ejecutados según una metodología de Proceso Analítico Jerárquico (APH)[4].

Estudio de localización para la instalación de PMI.

El estudio se basa en el análisis de la dinámica y expresión territorial de treinta indicadores, distribuidos en tres dimensiones y ponderados en función de una escala de tamaño de ciudades. Como resultado, se recomienda a las entidades federativas

[3] Esta sección sólo describe el proceso metodológico de los estudios. Para el modelo teórico, revise Apéndice 2 “Modelo de prevención situacional” del Anexo Técnico en su Capítulo 1.
[4] Para la descripción completa de la metodología APH, revise Apéndice 3 “Proceso analítico jerárquico para la elaboración de matriz de indicadores” del Anexo Técnico en su Capítulo 1.

identificar y contrastar los sitios que, en función de sus características socioeconómicas, de estructura urbana y de incidencia delictiva, deberían considerarse como prioritarios para la implementación de un Sistema de Vídeo Vigilancia que atienda a principios de prevención situacional del delito.

Tabla IV.1.1 Presentación general de dimensiones e indicadores del estudio de localización

PONDERACIÓN	DIMENSIONES	INDICADORES
Municipios Grandes (> 1,000,000) **Municipios Medianos (100 a 999 Mil)** **Municipios Pequeños (< 99,000)**	Socioeconómica	Densidad de Población
		Hacinamiento
		Estructura por Edad
		Rezago Social
		Tipo de Hogar
		Desigualdad Económica
		Nivel Socioeconómico
		Grado Promedio de Escolaridad
		Ocupación
		Cohesión Social
Municipios Grandes (> 1,000,000) **Municipios Medianos (100 a 999 Mil)** **Municipios Pequeños (< 99,000)**	Estructura Urbana	Concentración de Actividades Económicas
		Concentración de Personal Ocupado
		Equipamientos Educativos
		Equipamientos de Salud
		Otros Equipamientos
		Accesibilidad y Conectividad
		Cobertura de Alumbrado Público
		Cobertura de Pavimentación
		Cobertura de Banquetas
		Cobertura de Vegetación
Municipios Grandes (> 1,000,000) **Municipios Medianos (100 a 999 Mil)** **Municipios Pequeños (< 99,000)**	Incidencia Delictiva	Homicidios
		Violación
		Robo a Transeúnte con Violencia
		Robo a Transeúnte sin Violencia
		Robo a Vehículo Automotor con Violencia
		Robo a Vehículo Automotor sin Violencia
		Robo a Casa Habitación
		Robo a Negocio
		Robo a Transportistas
		Lesiones

Descripción y cálculo de indicadores.

A continuación, se describen los indicadores que se recomienda considerar, de manera enunciativa pero no limitativa, para obtener un estudio de localización para los PMI. No se omite mencionar que el desarrollo de este ejercicio permitirá contar con criterios cuantitativos y cualitativos para la toma de decisiones, basados en un modelo de prevención situacional que considera factores que tienen un grado de correlación con el acto delictivo.

Indicadores socioeconómicos.

a) *Densidad de población y vivienda.* La relación entre un espacio determinado y el número de personas que lo habitan se llama densidad de población, la cual se obtiene dividiendo el número de personas que viven en un lugar específico entre el número de kilómetros cuadrados o hectáreas que mide ese territorio, a nivel nacional la densidad de población es de 61 hab/km^2.

   Se debe distinguir la densidad bruta y la densidad absoluta, esta última refiere a la relación entre habitante y superficie urbana, mientras que la bruta corresponde a la superficie total de una unidad geográfica como estado o municipio en su totalidad.

b) *Hacinamiento.* Es la proporción de ocupantes de viviendas con más de tres personas por habitación. Determina la forma de coexistir de la población en cuanto a número de habitantes por vivienda particular habitada; considerando las viviendas con más de 3 habitantes por dormitorio sobre el total de viviendas, y de igual forma constituye la construcción del ambiente inmediato de convivencia.

   Para calcularlo, se presenta la fórmula y los valores comúnmente aceptados por los estudios demográficos:

Índice de Hacinamiento =
(Personas Habitando Una Vivienda) / (Número de Dormitorios en la Vivienda)

c) *Estructura por edad*. Representa la distribución relativa de la población según grandes grupos de edad y sexo. Se expresa en porcentaje. Se suelen clasificar tres grandes

grupos de edad: niños y jóvenes (G1: hasta los 14 años), adultos (G2: entre los 15 y 64 años) y los ancianos, (G3: mayores de 65 años).

Cálculo de los datos. Si los datos aparecen en números absolutos hay que hallar el porcentaje que corresponde a cada grupo de edad y sexo con respecto al total de la población. Para ello se deberá dividir la población de cada grupo de edad y sexo por la población absoluta y multiplicarlo por 100.

Porcentaje de Cada Grupo =
(Población de Cada Grupo x 100) / (Población Total)

Del mismo modo este análisis nos permite identificar los grupos dependiendo de la actividad que desarrollen:

- Población Transitoriamente Pasiva (PTP) está compuesta por los niños y niñas de entre 0 y 14 años que se supone no trabaja y se encuentran en proceso de formación bajo la tutela de sus padres o tutores.
- Población Activa (PA) está compuesta por los hombres y mujeres de entre 15 y 64 años que están en condiciones de trabajar en cualquier actividad económica.
- Población Pasiva Definitiva (PPD) comprende los hombres y mujeres que superan los 64 años de edad y ya no deberían trabajar. Este indicador muestra hacia donde se carga la pirámide de edades.

d) *Rezago social.* Índice que agrega variables de educación, de acceso a servicios de salud, de servicios básicos en la vivienda, de calidad y espacios en la misma, y de activos en el hogar. Es decir, proporciona el resumen de cuatro carencias sociales de la medición de pobreza del Consejo Nacional de Evaluación de la Política de desarrollo social (CONEVAL). Cabe destacar que no se trata de una medición de pobreza, ya que no incorpora los indicadores de ingreso, seguridad social y alimentación (CONEVAL, 2016).

e) *Hogares con jefatura femenina/ tipo de hogar.* Hogares en viviendas particulares habitadas donde el jefe de familia es mujer. Se considera un hogar en cada vivienda particular. Este índice muestra la distribución de los hogares con jefatura femenina.

f) *Desigualdad económica (Coeficiente de Gini).* Mide la distribución del ingreso respecto de una situación ideal en la que todos los individuos o familias de una comunidad obtienen un ingreso proporcional a su peso relativo en la distribución. Este indicador es una aproximación al análisis de la evolución de la distribución del ingreso y tiene consecuencias directas sobre los indicadores de pobreza.

La importancia de este indicador radica en su utilidad para identificar cambios en la distribución del ingreso y en el grado de desigualdad del mismo. Para identificar las zonas de mayor desigualdad el coeficiente se aproxima a 1 mientras cuando el coeficiente de se aproxima a 0 se tiende a una mayor mezcla de ingreso de la población para alcanzar un desarrollo incluyente.

g) *Nivel Socioeconómico.* La Asociación Mexicana de Inteligencia de Mercado y Opinión (AMAI), diseñó el índice de Niveles Socio Económicos (NSE) que agrupa los hogares en 6 niveles, de acuerdo a su capacidad de satisfacer necesidades básicas como educación, calidad de la vivienda, salud, acceso a medio tecnológicos, desarrollo intelectual, calidad de vida y bienestar. Para dicha clasificación, la AMAI definió 13 variables, considerando:

- Último año de estudios del jefe de familia.
- Número de focos en el hogar.
- Número de habitaciones sin contar baños.
- Número de baños con regadera dentro del hogar.

Posesión de:

- Autos (ya sean de su propiedad o no).
- Calentador de agua / Boiler.
- Tipo de piso (solamente de cemento o de otro material).
- Aspiradora.
- Computadora (PC).

- Horno de microondas.
- Lavadora de ropa.
- Tostador de Pan.

Con estas variables se asignaron seis niveles socioeconómicos diferentes.

Tabla IV.1.2 Clasificación de niveles socioeconómicos AMAI

NSE	CLASIFICACIÓN	CARACTERÍSTICAS
A/B	Clase Alta	Tiene cubiertas todas las necesidades de bienestar, es el segmento con más alto nivel de vida. El perfil del jefe de familia es nivel educativo de licenciatura o mayor. Único segmento que cuenta con recursos para invertir y planear para el futuro. Mayor proporción de gastos en educación, entretenimiento, comunicación, vehículos. Viven en departamentos o casas de lujo con todas las comodidades.
C+	Clase Media Alta	Segmento con ingresos y/o estilo de vida ligeramente superior a los de clase media. Los jefes de familia tienen un nivel educativo de licenciatura. Tiene cubiertas todas las necesidades de bienestar, presenta limitantes para invertir y ahorrar para el futuro. Mayor proporción de gastos en educación, entretenimiento, comunicación, vehículos. Generalmente viven en casas o departamentos propios, algunos de lujo, y cuentan con todas las comodidades.
C	Clase Media	Se caracteriza por tener un nivel de vida práctica y con ciertas comodidades. El perfil del jefe de familia cuenta con preparatoria. Aspira a mayor bienestar en entretenimiento y tecnología. Mayor proporción de gastos en educación, entretenimiento, comunicación, vehículos. Los hogares de este segmento son cosas o departamentos propios o rentados con algunas comodidades.
D+	Clase Media Baja	Segmento con ingresos y/o estilos de vida ligeramente menores a los de la clase media. El perfil del jefe de familia de estos hogares está formado por individuos con un nivel educativo de secundaria o primaria completa. Tiene cubierta la mínima infraestructura sanitara de su hogar; aspira a adquirir bienes y servicios que le hagan la vida más práctica y sencilla. Mayor proporción del gasto en alimentos, transporte y cuidado personal. En su mayoría las viviendas o departamentos de este segmento con de su propiedad, aunque algunas personas rentan el inmueble y algunas viviendas son de interés social.
D	Clase Baja	Tiene una propiedad o renta (generalmente en vecindades o viviendas de interés social), pero carece de la mayoría de servicios y bienes satisfactores, aspirando a contar con servicios sanitarios mínimos. La mayor proporción del gasto se aplica en alimentos, transporte y cuidado personal. El perfil del jefe de familia está formado por individuos con un nivel educativo de primaria completa en promedio.
E	Clase más baja	Carece de todos los servicios y bienes satisfactores, aspira a contar con una propiedad y servicios sanitarios mínimos; no cuentan con un lugar propio, teniendo que rentar o utilizar otros recursos, en un solo hogar suelen vivir más de una generación. Mayor proporción del gasto en alimentos, transporte y cuidado personal. El jefe de familia se caracteriza por tener un nivel educativo de primaria inconclusa.

h) *Nivel educativo promedio.* Es el número de años que en promedio aprobaron las personas de 15 años y más en el Sistema Educativo Nacional; es el resultado de dividir la suma de los años aprobados desde el primer año de primaria hasta el último grado alcanzado de las personas de 15 y más años, entre el total de la población de 15 y más años, esta medición excluye a las personas que no especifican los grados aprobados.

Se utiliza como dato complementario para conocer las capacidades de la población de un determinado lugar y las posibilidades que ésta tiene para incorporarse en el mercado de trabajo.

$$\frac{\sum\left(P^{S}_{N\ (15\ y\ más)}\right)(N)}{P^{S}_{(15\ y\ más)} - NE}$$

Donde:

$P^{S}_{N\ (15\ y\ más)}$	Población de 15 y más años de sexo S con N años de estudio aprobados.
$P^{S}_{(15\ y\ más)}$	Población total de 15 y más años de sexo S.
N	Número de años de estudio aprobados.
NE	No especificado.
S	Hombres, mujeres.

Tabla IV.1.3 Nivel de escolaridad

NIVEL DE INSTRUCCIÓN		AÑOS ACUMULADOS (GRADO DE ESCOLARIDAD)
Sin instrucción	n/a	0
Primaria	1°	1
	2°	2
	3°	3
	4°	4
	5°	5
	6°	6
Estudios técnicos o comerciales con primaria terminada y secundaria.	1°	7
	2°	8
	3°	9
Preparatoria, estudios técnicos o comerciales con secundaria terminada y normal básica.	1°	10
	2°	11
	3°	12
	4°	13

Fuente: INEGI http://cuentame.inegi.org.mx/poblacion/escolaridad.aspx?tema=P

i) *Ocupación.* La Tasa de Desocupación Abierta es la proporción de personas que desean trabajar y están en condiciones legales de hacerlo, pero no encuentran empleo. También refiere al porcentaje de la población desocupada con respecto al total de la población económicamente activa.

Se obtiene al dividir la Población Desempleada entre la Población Económicamente Activa (PEA) y el resultado multiplicarlo por 100.

$$(Pd/\ PEA)*100$$

Donde:
Pd: población desocupada.
PEA: población económicamente activa.

j) *Cohesión social.* La medición de la cohesión social adoptada por CONEVAL incorpora indicadores que ayudan a conocer la desigualdad económica y social a nivel nacional, estatal y municipal, e indicadores de redes de apoyo e intercambio social a nivel estatal. Para medir el grado de cohesión social, el CONEVAL utiliza cuatro indicadores, para ofrecer los resultados a nivel estatal y municipal, clasificándolos en alta y baja cohesión:

- Coeficiente de Gini.
- Razón de ingreso.
- Grado de Polarización social.
- Índice de percepción en redes sociales.

Indicadores de la Estructura Urbana.

a) *Concentración de actividades económicas.* Existe una relación directa entre el espacio, la actividad delictiva y las actividades económicas (comercio y servicios). Las concentraciones de actividades económicas y su distribución en el territorio pueden influenciar en el dinamismo del lugar, propiciando un alto nivel de tránsito peatonal y de actividades complementarias. Siguiendo la lógica de los delitos de oportunidad, la

recomendación a partir del reconocimiento de concentraciones es ubicar estratégicamente cámaras en estos puntos.

b) *Concentración de personal ocupado.* La concentración de personal ocupado es el referente a la distribución de las unidades económicas pero respecto a su tamaño, ya que pueden existir zonas con muchas unidades económicas pero estas solo tienen de 1 a 2 empleados en cada una o puede existir solo 2 o 3 unidades económicas pero con una concentran de más de 750 empleados cada una.

c) *Equipamientos educativos.* Los equipamientos educativos constituyen bienes públicos que garantizan a la población el acceso a servicios tendientes a cubrir sus necesidades de educación; lo que, en función de su distribución espacial puede fomentar la coexistencia de una estructura social diversa, el fortalecimiento del tejido social y generar niveles de calidad material y ambiental que procuren satisfacción a la población. La cobertura del equipamiento educativo es fundamental para el desarrollo social y económico.

Para el cálculo del equipamiento educativo se considera la cobertura espacial de todos los equipamientos en un lugar dado (Porcentaje de cobertura en el territorio).

d) *Equipamientos de salud.* El uso y apropiación del equipamiento urbano permite que el ciudadano estructure su conocimiento del entorno urbano y se integre a su comunidad. La cobertura del equipamiento salud es un factor determinante del bienestar social.

Para el cálculo del equipamiento de salud se considera la cobertura espacial de todos los equipamientos en un lugar dado (Porcentaje de cobertura en el territorio).

e) *Equipamientos otros.* El uso y apropiación del equipamiento urbano permite que el ciudadano estructure su conocimiento del entorno urbano y se integre a su comunidad. Los equipamientos constituyen bienes públicos que permiten garantizar a la población el acceso a satisfactores que contribuyen al bienestar de la población.

Equipamientos como espacios, abiertos y parques y jardines son factores que generan cohesión social, propicia la comunicación, interrelación e integración de la comunidad.

Para el cálculo del equipamiento otros se consideran la cobertura espacial de todos los equipamientos (Espacio público, parques, jardines, juegos infantiles, deportivos, etc.) en un lugar dado (Porcentaje de cobertura en el territorio).

f) *Accesibilidad - conectividad.* La accesibilidad es la facilidad que tiene la población para alcanzar las oportunidades (destinos) distribuidas en el territorio desde cualquier otro punto (orígenes), empleando la red de infraestructura para transporte público y transporte privado. La conectividad y la accesibilidad se calculan con la estructura vial de la ciudad por medio de ejes axiales. Los resultados se valoran de 0 a 1 donde 1 tiene un muy alto nivel de accesibilidad-conectividad y 0 muy bajo nivel de accesibilidad-conectividad.

g) *Cobertura de alumbrado público.* *R*efiere a la cobertura de alumbrado público, de tal manera que se mide el porcentaje de manzanas en una unidad de análisis que cuenta con dichos servicios.

$$\% \, CS = \frac{P \times 100}{TM}$$

Donde:
CS: Cobertura del servicio.
P: manzanas que cuentan con el servicio.
TM: Total de manzanas.

Se puede considerar el nivel de cobertura en función de la siguiente escala:

Bueno	≥90%
Regular	50-90%
Malo	<50%

h) *Cobertura de pavimentación.* Este indicador refiere a la cobertura de pavimentación, de tal manera que se mide el porcentaje de manzanas en una unidad de análisis que cuenta con dichos servicios.

$$\% \, CS = \frac{P \times 100}{TM}$$

Donde:

CS: Cobertura del servicio.
P: manzanas que cuentan con el servicio.
TM: Total de manzanas.

Se puede considerar el nivel de cobertura en función de la siguiente escala:

Bueno	≥90%
Regular	50-90%
Malo	<50%

i) *Cobertura banquetas.* Este indicador refiere a la cobertura de banquetas, de tal manera que se mide el porcentaje de manzanas en una unidad de análisis que cuenta con dichos servicios.

$$\% \, CS = \frac{P \times 100}{TM}$$

Donde:
CS: Cobertura del servicio
P: manzanas que cuentan con el servicio
TM: Total de manzanas

Se puede considerar el nivel de cobertura en función de la siguiente escala:

Bueno	≥90%

Regular	50-90%
Malo	<50%

j) *Cobertura de vegetación.* Este indicador refiere a la cobertura de vegetación, de tal manera que se mide el porcentaje de manzanas en una unidad de análisis que cuenta con dichos servicios.

$$\% \, CS = \frac{P \times 100}{TM}$$

Donde:
CS: Cobertura del servicio
P: manzanas que cuentan con el servicio
TM: Total de manzanas

Se puede considerar el nivel de cobertura en función de la siguiente escala:

Bueno	≥90%
Regular	50-90%
Malo	<50%

Incidencia Delictiva.

Las variables delictivas son calculadas a partir de tres razones: por concentración de delitos por hectáreas; según su tasa delictiva y, finalmente, por análisis de Hot-Spot.

Dentro de la matriz de dimensión delictiva se incorporara solamente las de concentración de delitos por hectárea.

a) *Concentración de delitos por hectárea*. Es la distribución del número de delitos en una unidad de análisis territorial (país, estado, distrito, AGEB, etc.) y se calcula dividiendo la cantidad total de delitos entre la superficie, en este caso expresada en hectáreas.

$$CD = DT/Sup$$

Donde:

CD: Cantidad de delitos.

DT: Delitos totales.

Sup: Superficie sectorial.

b) *Tasa delictiva.* Es la cantidad de delitos por cada 100,000 habitantes en un área. Se calcula dividiendo la cantidad de delitos de un perímetro determinado entre su población multiplicado por 100,000.

$$Dph= (DT/Pob\ Tot)*100,000$$

Donde:

Dph: Delitos por cada 100 mil habitantes.

DT: Delitos totales.

Pob Tot: Población total.

c) *Análisis de la densidad delictiva (Hot Spot).* Los Sistemas de Información Geográfica (SIG) permiten profundizar en el comportamiento del delito en el territorio a través de su localización puntual en el espacio. Un *Hot Spot* refiere a un punto conflictivo, donde se concentra una mayor densidad de delitos.

Los mapas *hotspot* son útiles para identificar visualmente la concentración de delitos en un radio de alcance establecido por el analista (250 a 500 m), así como establecer patrones e identificar la posibilidad de ocurrencia de ciertos delitos.

Mediante el uso de un SIG se puede calcular el centro principal de una actividad delictiva, a través del promedio de las coordenadas en "*x*" y "*y*" de cada uno de los hechos delictivos ocurridos en determinada zona.

Los indicadores antes expuestos, podrán ser utilizados por la entidades federativas como una guía o punto de referencia sobre la localización de los PMI.

Matriz de ponderación por área de análisis.

Este apartado presenta una matriz de ponderación, donde se jerarquizará la información obtenida a partir del análisis espacial de los indicadores recomendados. Como resultado, las entidades interesadas en implementar un Sistema de Vídeo Vigilancia podrán determinar las zonas prioritarias que, en función de sus características socioeconómicas, de estructura urbana e incidencia delictiva, tendrán un mayor impacto preventivo sobre la problemática de inseguridad que los afecta.[5]

Matriz de escenarios de localización.

Una vez que se haya establecido el comportamiento de los indicadores a partir de la matriz de ponderación por área de análisis, se lleva a cabo la construcción de la ponderación de importancia para cada uno de estos. Para ello, se propone una evaluación promedio en un rango del 0 al 1 donde uno es el indicador menos importante y 0 el más importante.

En la matriz, al final de cada columna de ciudades *Grandes, Medias y Pequeñas*, se establecerán los valores máximos y mínimos según la ponderación.

$$SSV = \sum_{i}^{n} Xi * b$$

Donde:
SSV: Presencia de cámaras de video vigilancia
X: es la variable de ponderación
B: es la constante del tipo de ciudad

De esta forma los 30 indicadores propuestos serán ponderados para cada uno de los rangos de ciudad.

[5] Para la implementación de este ejercicio, el analista deberá utilizar las matrices que integran el Apéndice 4 “Mátrices de ponderación por áreas de análisis” del Anexo Técnico en su Capítulo 1.

Tabla IV.1.4 Matriz de escenarios de localización

Dimensiones	SOCIO-ECONÓMICA	ESTRUCTURA URBANA	INCIDENCIA DELICTIVA
Pesos	0.3	0.3	0.4
Municipios grandes > 1,000,000	0 - .3	0 - .3	0 - .3
	.3 - .7	.3 - .7	.3 - .7
	.7 - 1	.7 – 1	.7 - 1
Municipios medianos 100,000-999,000	0 - .3	0 - .3	0 - .3
	.3 - .5	.3 - .5	.3 - .5
	.5 - 1	.5 – 1	.5 - 1
Municipios pequeños < 99,999	0 - .4	0 - .4	0 - .4
	.4 - .6	.4 - .6	.4 - .6
	.6 - 1	.6 – 1	.6 - 1

Si los valores obtenidos en la sumatoria cubren estos rangos tendremos:

Tabla IV.1.5 Sistema de vídeo vigilancia recomendado

ESCENARIO	1. GRANDE	2. MEDIA	3. PEQUEÑA	RECOMENDACIÓN DE LOCALIZACIÓN DE SSV
ALTO IMPACTO	0.7 - 1	0.8 - 1	0.8 - 1	**PRIORITARIO**
MEDIO IMPACTO	0.5 – 0.7	0.6 – 0.8	0.5 – 0.8	**RELEVANTE**
BAJO IMPACTO	0 – 0.5	0 – 0.6	0 – 0.5	**NO RECOMENDABLE**

Estudio de densidades para la instalación de PMI.

El cálculo de las densidades de los postes se obtiene por medio de los pesos ponderados de las tres dimensiones: socio-económica, estructura urbana e incidencia delictiva; el resultante es una recomendación de la densidad deseada de los sistemas de video vigilancia. Complementariamente, se utiliza una clasificación de tres tipos de morfología urbana[6] para ajustar los patrones de densidad, considerando que según su clasificación algunas trazas ofrecen mejores o peores condiciones de visualización; por ejemplo:

[6] Para profundizar en las características de la tipología de morfologías urbanas, ver Apéndice 5 "Caracterización de la morfología urbana" del Anexo Técnico en su Capítulo 1.

1. **Trazas ortogonales**, el campo visual suele ser mayor, por tal motivo pueden tener una menor densidad de PMI (mayor esparcimiento territorial).

2. **Trazas irregulares:** Cuya visual se ve interrumpida por las características de continuidad no ortogonal y si del tipo llamado "plato roto".

3. **Traza llamadas orgánicas**: Cuyo campo visual es menor por las líneas curvas y senderos oblicuos, cuya circunstancia requiere de densidades de postes diferenciales.

Construcción de las variables.

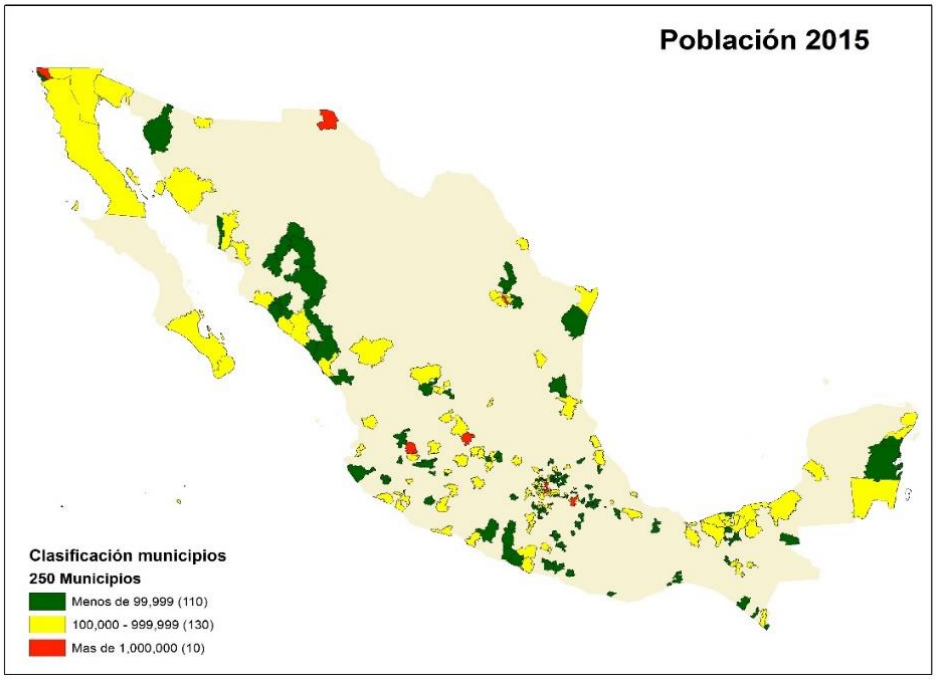
Tamaño del municipio.

Para determinar el escenario "Tamaño de municipio" se determinara de acuerdo con los siguientes rangos:

- Menos de 99,999 habitantes
- 100,000 a 999,999 habitantes
- Más de 1, 000,000 habitantes

De los 2,456 municipios que conforman la República Mexicana, el CNI definió como prioritarios 250 municipios mediante un análisis estadístico de la incidencia delictiva que pondera el nivel de incidencia delictiva y la tasa de crecimiento.

Mapa IV.1.2 Municipios prioritarios de acuerdo al CNI distribuidos en tres rangos propuestos



Fuente: Elaboración propia con base en información del INEGI, Encuesta Intercensal 2015

Densidad poblacional.

La densidad poblacional juega un papel importante en la determinación de la colocación de los sistemas de video vigilancia. A altas densidades poblacionales pueden corresponder mayores niveles de incidencia delictiva. Esto debido a dos condicionantes, la primera a la cuestión de que hay mayor cantidad de gente por unidad terrotorial, y el segundo factor es de carácter psicológico y responde al factor del espacio interpersonal y los conflictos derivados de ello.

Para determinar los parámetros de densidades poblacionales se parte del hecho de que existen tres niveles de análisis que están referidos al tamaño de municipio (Grandes, medianos y pequeños), y a partir de éstos se construyen tres tipos de escenarios por el grado de densidad poblacional.

Tabla IV.1.6 Densidad poblacional

Tamaño de municipio	Densidad poblacional		
	Alta	**Media**	**Baja**
Municipios Grandes	> 250 Hab/ha .35	150 - 250 Hab/ha .33	< 150 Hab/ha .30
Municipios medianos	>200 Hab/ha .33	100 - 200 Hab/ha .31	< 100 Hab/ha .29
Municipios pequeños	>150 Hab/ha .31	75 - 150 Hab/ha .29	< 75 Hab/ha .28

Para la obtención del nivel de densidad poblacional se deberá generar un plano a nivel de AGEB donde se muestren las densidades poblacionales y ubicar la zona de implementación de los sistemas de video vigilancia. A partir de ello se deben obtener los valores de la densidad poblacional, ya sea de una sola AGEB donde se extraería el valor mostrado; o si la zona está compuesta de varias AGEBs, se obtendría el promedio de densidad poblacional.

A partir de obtener la densidad poblacional hay que remitirse a la Tabla IV.1.6 (Densidad poblacional), donde se identificará primero el tipo de municipio y segundo el nivel de densidad poblacional, en dicho recuadro se obtendrá el primer valor ponderado de los tres valores que se necesitan para ubicar la densidad de postes que se requiere para dicha zona.

Concentración de unidades económicas.

La concentración de unidades es otro factor primordial para la ubicación y colocación de los sistemas de video vigilancia, ya que existe una correlación espacial muy alta entre la alta incidencia delictiva y la alta concentración de unidades económicas.

Esta correlación espacial se presenta principalmente en los centros, subcentros y corredores urbanos donde se concentran la mayor cantidad de unidades económicas dentro del contexto urbano.

Para determinar los parámetros de concentración de unidades económicas se parte del hecho de que existen tres niveles de análisis del tamaño de municipio: 1) grandes, 2) medianos y 3) pequeños. A partir de éstos, se construyen tres tipos de escenarios por el grado de concentración de unidades económicas:

Tabla IV.1.7 Concentración de unidades económicas

Tamaño de municipio	Concentración unidades económicas .25		
	Alta	**Media**	**Baja**
Municipios Grandes	>500 UE .25	300-500 UE .23	< 300 UE .22
Municipios medianos	>300 UE .23	200-300 UE .22	< 200 UE .21
Municipios pequeños	>200 UE .22	100-200 UE .21	< 100 UE .20

Para la obtención del nivel de concentración de unidades económicas, se deberá generar un plano a nivel de AGEB donde se muestren la concentración de unidades económicas y ubicar la zona de implementación de los sistemas de video vigilancia. A partir de ello, se deberán obtener los valores de la concentración de unidades económicas, ya sea de una sola AGEB donde se extraería el valor mostrado, o si la zona está compuesta de varias AGEBs, se obtendría el promedio de la concentración de unidades económicas.

Una vez obtenida la concentración de unidades económicas, hay que remitirse a la Tabla IV.1.7 (Concentración de unidades económicas), donde se identificará primero el tipo de municipio y, segundo el nivel de concentración de unidades económicas. En dicho recuadro se obtendrá el segundo valor ponderado de los tres valores que se necesitan para ubicar la densidad de postes para una determinada zona.

Concentración de delitos.

Como tercera variable en de la ponderación final se tiene la concentración de delitos por hectárea. Esta es la variable con mayor peso dentro de la ponderación final, por la importancia y la pertinencia para la localización de los sistemas de video vigilancia.

Para determinar los parámetros de concentración de incidencia delictiva se parte del hecho de que existen tres niveles de análisis determinados por el tamaño de municipio: grandes, medianos y pequeños. A partir de éstos, se construyen los tipos de escenarios por el grado de concentración de incidencia delictiva:

Tabla IV.1.8 Concentración de incidencia delictiva

Tamaño de municipio	Concentración incidencia delictiva .40		
	Alta	**Media**	**Baja**
Municipios Grandes	>40 Da .40	20-40 D .38	<20 Da .36
Municipios medianos	>35 D .38	25-35 .36	<25 D .34
Municipios pequeños	>30 D .36	30-20 D .34	<20 D .32

Para la obtención del nivel de concentración de incidencia delictiva se deberá generar un plano a nivel de AGEB donde se muestren la concentración de incidencia delictiva y ubicar la zona de implementación de los sistemas de video vigilancia. A partir de ahí, se obtienen los valores de la concentración de incidencia delictiva, ya sea de una sola AGEB donde se extraería el valor mostrado, o si la zona está compuesta de varias AGEBs, se obtendría el promedio de la concentración de incidencia delictiva.

A partir de obtener la concentración de incidencia delictiva, hay que remitirse a la Tabla IV.1.8 (Concentración de incidencia delictiva) donde se identificará primero el tipo de municipio y segundo el nivel de concentración de incidencia delictiva. En dicho recuadro se obtendrá el segundo valor ponderado de los tres valores que se necesitan para ubicar la densidad de postes que se requiere para dicha zona.

Para finalizar, se hace la sumatoria de las variables de densidad poblacional, concentración de unidades económicas y concentración de incidencia delictiva, ubicándolas en el tipo de tamaño de municipio para clasificar y obtener el índice de densidad de postes para la implementación de los Sistemas de Video Vigilancia.

Complementariamente, se utiliza una clasificación de tres tipos de morfología urbana[7] para ajustar los patrones de densidad, considerando que según su clasificación, algunas trazas ofrecen mejores o peores condiciones de visualización. En trazas ortogonales, el campo visual suele ser mayor, por tal motivo pueden tener una menor densidad de PMI (mayor esparcimiento territorial). Por el contrario, en trazas irregulares y orgánicas, el campo visual es menor por tal motivo se necesitan densidades mayores de postes.

Los rangos de densidades de postes presentados en la Tabla IV.1.9, resultaron del análisis comparativo interestatal e intermunicipal, a partir de la información brindada por las Centros de Control visitados durante la etapa de diagnóstico.

Tabla IV.1.9 Criterios para la determinación de la Densidad Bruta de PMI, determinadas por AGEB.

	Densidad poblacional	Unidades económicas	Concentración de delitos (Alto impacto)	Morfología	Densidad de postes
Ciudades Grandes					
Alta	> 250 Hab/ha	>500 UE/Ha	>40 D/Ha	Ortogonal	1 c/13 Ha
				Irregular	1 c/12 Ha
				Orgánica	1 c/10 Ha
Media	150 - 250 Hab/ha	300-500 UE/Ha	20-40 D/Ha	Ortogonal	1 c/19 Ha
				Irregular	1 c/18 Ha
				Orgánica	1 c/16 Ha
Baja	< 150 Hab/ha	< 300 UE/Ha	<20 D/Ha	Ortogonal	1 c/21 Ha
				Irregular	1 c/20 Ha
				Orgánica	1 c/18 Ha
Ciudades medianas					
Alta	>200 Hab/ha	>300 UE/Ha	>35 D/Ha	Ortogonal	1 c/16 Ha
				Irregular	1 c/15 Ha
				Orgánica	1 c/13 Ha
Media	100 - 200 Hab/ha	200-300 UE/Ha	25-35 D/Ha	Ortogonal	1 c/18 Ha
				Irregular	1 c/17 Ha
				Orgánica	1 c/15 Ha
Baja	< 100 Hab/ha	< 200 UE/Ha	<25 D/Ha	Ortogonal	1 c/23 Ha
				Irregular	1 c/22 Ha
				Orgánica	1 c/20 Ha

[7] Para profundizar en las características de la tipología de morfologías urbanas, ver Apéndice 5 "Caracterización de la morfología urbana" del Anexo Técnico en su Capítulo 1.

Ciudades pequeñas					
Alta	>150 Hab/ha	>200 UE/Ha	>30 D/Ha	Ortogonal	1 c/18 Ha
				Irregular	1 c/17 Ha
				Orgánica	1 c/15 Ha
Media	75 - 150 Hab/ha	100-200 UE/Ha	30-20 D/Ha	Ortogonal	1 c/20 Ha
				Irregular	1 c/19 Ha
				Orgánica	1 c/17 Ha
Baja	< 75 Hab/ha	< 100 UE/Ha	<20 D/Ha	Ortogonal	1 c/22 Ha
				Irregular	1 c/21 Ha
				Orgánica	1 c/19 Ha

Delimitación de la zona de aplicación de la localización de los sistemas de video vigilancia

Una vez que se obtienen las densidades, se generan los polígonos de aplicación para los sistemas de video vigilancia. Para la identificación de dichos polígonos, se toma como el principal factor para su delimitación, las zonas de mayor concentración de incidencia delictiva, y estas serán generadas e identificadas por medio de análisis de *hotspots*.

Los *hotspots* son áreas en un mapa que tiene la mayor concentración de delitos. Para generar estas zonas se deberá de contar con los delitos registrados y capturados cartográficamente en forma de puntos en un sistema de información geográfica.

Existen diferentes herramientas para generar el *hotspot* y la más común es la técnica de “Distancia al vecino más cercano”. Esta herramienta genera un análisis de agrupamiento.

Este análisis da la opción de aplicar un parámetro de distanciamiento entre delito y delito. Por predeterminado, se aplicará una distancia de 500 metros (la distancia promedio caminable para cada persona). Si la distancia entre delito y delito es menor de 500 metros, los delitos tenderán a agruparse, mientras que los delitos que estén a mayor distancia, estos no suman a las zonas de mayor concentración.

Para el cálculo de *hotspot*, los programas de Sistemas de Información Geográfica incorporan una herramientas para generarlo. Solamente se deberá proporcionar el parámetro de esparcimiento (500 metros, en este caso).

Una vez generado el plano de *hotspots,* será posible identificar las zonas de mayor concentración de delitos. Con este plano, se delimitarán las zonas que estén por encima de la media. Se clasificará en cinco rangos por medio del método de *natural breaks*, teniendo como resultado los dos últimos rangos como zonas de aplicación para colocar los Sistemas de Video Vigilancia.

Conclusión

Por último, es importante considerar la diferencia que representa la densidad bruta de postes con relación a la densidad neta, ya que la primera tendrá que ser calculada con base en la superficie urbana total (en cuyo caso se aplican los criterios expuestos en la tabla VI.1.9 Densidad Bruta de PMI, determinadas por AGEB). A diferencia de la densidad neta que está referida al número de postes por hectárea dentro en un territorio donde se concentra la actividad delictiva (hotspot).

El cálculo de la densidad neta de postes para un determinado territorio se deberá realizar a partir de la información específica de la concentración de delitos en cada localidad. A partir de datos obtenidos en el estudio de campo se puede estimar que la concentración neta de postes en un territorio de mayor concentración delictiva (*hotspot*) puede llegar hasta a un 90 % del total calculado para la densidad bruta.

IV.2 Diseño de Postes y Cimentaciones

IV.2.1 Justificación

Una vez que se ha analizado cómo determinar la localización y la densidad de los nodos del sistema de video vigilancia, es indispensable conocer cuál es el alcance de esta Norma en término de las especificaciones técnicas de la infraestructura. Como se ha mostrado en el apartado anterior, la implementación adecuado no depende únicamente de factores como la densidad poblacional o la densidad delictiva; aspectos físicos como la morfología de las ciudades deben tomarse en cuenta para un aprovechamiento óptimo de la inversión.

En este apartado se establecen, de forma general, las especificaciones relevantes para los postes de video vigilancia, en términos de su diseño, cimentación y estructura, así como su implementación e instalación en campo. Características como la geografía del municipio o estado, topográfica, tipo de suelo, clasificación de estructura, altura de la estructura, grado de seguridad estructural, zona sísmica y velocidad del viento, son factores a considerar.

Asimismo, el diseño de las cimentaciones cobra gran importancia para establecer condiciones y especificaciones mínimas necesarias sobre el suelo y subsuelo, sobre todo, ante condiciones meteorológicas adversas, movimientos telúricos y/o impacto eólico. Así para determinar la seguridad estructural, se considera el diseño del poste en función del coeficiente sísmico de la zona y la velocidad del viento.

En cuanto a la altura de los postes de objetivos de mayor nitidez, se toma en cuenta su función de observación respecto a estructuras como escuelas, parques, centros comerciales, oficinas de gobierno, hospitales, puntos de alta concurrencia, entre otros. Tampoco debe olvidarse que la altura del poste debe ser pensada también desde su visibilidad a nivel de calle, especialmente en espacios públicos donde se busque el inhibición del delito a través de la presencia de SVV.

La observancia de este apartado en el diseño e implementación de los SVV debe ser estricta, en función de que la inversión realizada corresponda con los estándares de construcción y respete las condiciones geográficas y topográficas. De no tomarse en consideración, se corre el riesgo de que los postes de SVV sean un peligro para la integridad de los ciudadanos en momentos de sismo o desastres naturales, no solo anulando su utilidad en la prevención de siniestros, sino convirtiéndose en una vulnerabilidad mayor para las urbes.

IV.2.2 Glosario

Para contextualizar la información en el ámbito de la presente Norma, se presenta a continuación un glosario de términos y definiciones relacionadas.

- A.I.S.C: Instituto Americano de la Construcción en Acero.
- A.S.C.E: American Society of Civil Engineers.
- A.S.T.M: American Society for Testing Materials.
- Aref: Área de referencia sobre la que actúa la presión, en m^2.
- Az: Área de la estructura, o parte de ella, sobre la que actúa la presión de diseño, pz, en m^2.
- C: Coeficiente de escala de rugosidad, adimensional.
- CI: Costo inicial de la construcción.
- Compresión simple o axial: Prueba especial de laboratorio, se usa para estimar la cohesión de los materiales.
- Compresión triaxial: Prueba especial usada para determinar las características de esfuerzo deformación y de resistencia de los suelos.
- Consolidación unidimensional: Prueba especial que permite determinar los asentamientos totales de una obra dada y prever la evaluación de los asentamientos con el tiempo.
- Contracción lineal: Prueba para determinar la contracción de un suelo, que consiste en realizar mediciones de la longitud y peso de un prisma, hasta que no se observe ninguna disminución de la longitud.

- CL: Costo de las reparaciones y de las pérdidas directas e indirectas que se tendrían en caso de una falla estructural.
- Cp: Coeficiente de presión, adimensional.
- Estado límite de falla: La resistencia del diseño de la estructura de toda la sección con respecto a cada fuerza actuante interna, debe de ser igual o mayor que el valor de diseño.
- Estado límite de servicio: La resistencia de la estructura ante deformaciones o agrietamientos deben de estar limitadas a valores tales que permita el funcionamiento en condiciones de servicio satisfactorio.
- Estratigrafía: Elemento gráfico que define la descripción de las capas componentes del subsuelo, su profundidad, su espesor y Algunas de sus propiedades.
- Exploración: Acción que se realiza con la finalidad de determinar las condiciones del subsuelo y sus propiedades físicas, índice y Mecánicas, ejecutado in situ, mediante observaciones directas o sondeos.
- F_{AD}: Factor de amplificación dinámica, adimensional.
- F_{eq}: Fuerza equivalente dinámica, en N.
- F_{es}: Fuerza estática, en N.
- F_{rz}: Factor de exposición local, adimensional.
- F_T: Factor de topografía local, adimensional.
- G: Factor de corrección por temperatura y por altura con respecto al nivel del mar, adimensional.
- Geotecnia: Técnicas de evaluación del comportamiento de los suelos, bajo la solicitación de cargas y bajo el ataque de los Agentes atmosféricos.
- Granulometría: Se denomina a la clasificación granulométrica de la medición y graduación de los granos de los materiales sedimentarios, de los suelos previstos por una escala granulométrica.
- Ht: Altura del promontorio o terraplén, medida verticalmente desde el inicio de la cuesta hasta la cresta, en m.
- Hm: Altura sobre el nivel del mar, en m.
- I.M.C.A: Manual de Construcción en Acero del Instituto Mexicano de la Construcción en Acero
- Índices de consistencia:

- Kgf: Unidad de medida Kilogramo fuerza
- Laboratorio de Geotecnia: Realiza los trabajos correspondientes a las pruebas para determinar las características físicas-mecánicas de un suelo o roca, mediante aplicación de una metodología aceptada y con los equipos e instrumentos apropiados en una muestra representativa.
- Levantamiento Topográfico: Son el conjunto de actividades para recabar en campo con los instrumentos y equipos apropiados, los datos necesarios para reproducir en dibujo a escala, una extensión de terreno ya sea en proyección horizontal, vertical o ambas.
- Límites de consistencia o atterberg: Se le denomina al conjunto de estados de consistencia de los materiales plásticos, provocados por el contenido de agua.
- L_1: Escala longitudinal para determinar la variación vertical de F_T, en m.
- L_2: Escala longitudinal para determinar la variación horizontal de F_T, en m.
- Lodo bentonitico: Mezcla de agua con bentonita, auxiliar en la perforación mediante equipo rotario, que sirve para estabilizar las paredes de sondeos.
- Ls: Distancia horizontal de la zona de separación del flujo, en m.
- Lu: Distancia horizontal en barlovento medida desde Ht /2 hasta la cresta del promontorio o terraplén, en m.
- Métodos geofísicos: Métodos de exploración que se realizan utilizando fenómenos físicos, tales como la gravedad de la tierra, ondas Sísmicas, resistividad y el magnetismo de la tierra.
- Muestra: Material de suelo o roca tomada con propósito de estudio en un laboratorio de mecánica de suelos.
- Muestreo: Es el método de exploración directa para obtener muestras de suelo apropiadas para la realización de las pruebas de laboratorio.
- Muestras Alteradas: Si a causa del procedimiento de extracción se pierde el acomodo original de las partículas del suelo.
- Muestras Inalteradas: Son aquellas cuya estructura no se modifica significativamente al ser extraídas.
- Penetración Estándar: El ensayo de penetración estándar o SPT (del inglés Standard Penetration Test), es una prueba de penetración dinámica, empleada para ensayar terrenos en los que se quiere realizar un reconocimiento geotécnico.

- Permeabilidad: Es la capacidad que tiene el suelo de permitirle a un flujo que lo atraviese sin alterar su estructura interna, dejando pasar a través de él una cantidad apreciable de fluido en un tiempo dado.
- Peso Volumétrico:
- Propiedades físicas y mecánicas: Las propiedades físicas de los materiales son las que describen el estado que guarda las partículas componentes del Suelo, que definen su apariencia. Las mecánicas son las que describen el comportamiento de los suelos bajo Esfuerzos inducidos y cambios del medio ambiente.
- Propiedades índice: Son propiedades útiles para la clasificación de los suelos cohesivos y proveen correlaciones con las propiedades Mecánicas de los suelos.
- p_z: Presión actuante sobre una construcción, en Pa.
- Prueba de penetración estándar: Método de exploración de suelos que consiste en hincar un penetrómetro mediante el golpeo de un martinete, donde el número de golpes es el parámetro principal para calcular el esfuerzo cortante de los suelos estudiados.
- Q: Relación entre el costo de las pérdidas al ocurrir una falla estructural y el costo inicial de la construcción, adimensional.
- q_z: Presión dinámica de base a una altura z sobre el nivel del terreno, en Pa.
- Sismicidad: Grado de frecuencia o de intensidad de los sismos que ocurre lugar en una zona determinada.
- SPT: Prueba de Penetración Estándar (Standard Penetration Test).
- SUCS: Sistema Unificado de Clasificación de Suelos.
- T: Periodo de retorno de la velocidad regional, VR, en años.
- Trabajos de Laboratorio: Para materiales de construcción se realizan pruebas para conocer las propiedades físicas y mecánicas de un material natural o procesado que se utilice en la construcción, mediante la aplicación de probeta representativa de ese material.
- Tubo de pared delgada: Herramienta para muestrear suelos.
- V_D: Velocidad básica de diseño, en km/h.
- V_R: Velocidad regional de ráfaga, en km/h.
- V_{RO}: Velocidad regional óptima de ráfaga, en km/h.
- VRS: Valor relativo de soporte

- Xt: Distancia horizontal en barlovento o sotavento, medida entre la estructura y la cresta del promontorio o terraplén, en m.
- Z: Altura sobre el nivel del terreno natural, a la que se desea conocer la velocidad de diseño, en m.
- Zt: Altura de referencia de la estructura medida desde el nivel promedio del terreno, en m.

Símbolos griegos:

- α: Exponente que determina la forma de la variación de la velocidad del viento con la altura, adimensional.
- δ: Altura gradiente, en m.
- τ: Temperatura ambiental, en ºC.
- Ω: Presión barométrica, en mm de Hg.

IV.2.3 Lineamientos normativos.

IV.2.3.1 Especificaciones Técnicas para el Diseño de Cimentación del Poste.

Exploración Geotécnica y Estudio de Mecánica de Suelos.

Las investigaciones y estudios del subsuelo a realizar, serán los mínimos necesarios que se requieran, para determinar las propiedades mecánicas del suelo y las condiciones del subsuelo se describen de manera específica en el Apéndice 1 “Postes” del Anexo Técnico en su Capítulo 2.

El número mínimo de exploraciones a realizar (pozos a cielo abierto o sondeos) será de uno por cada 80 m o fracción del perímetro o envolvente para las estructuras que se encuentren en suelos tipo lacustre y de transición o zonas I y II de acuerdo al Apéndice 1 “Postes” del Anexo Técnico en su Capítulo 2.

a) El número mínimo de exploraciones a realizar (pozos a cielo abierto o sondeos) será de uno por cada 120 m o fracción de dicho perímetro en los suelos tipo lacustre o zona III de acuerdo al Apéndice 1.

b) La profundidad de las exploraciones dependerá del tipo de cimentación y de las condiciones del subsuelo pero no será inferior a 2m bajo el nivel de desplante de la estructura.

c) Los sondeos que se realicen con el propósito de explorar el espesor de los materiales compresibles en los suelos de transición y lacustres (Zonas II y III) deberán, además, penetrar en el estrato incompresible al menos 3 m.

d) Los procedimientos para localizar rellenos artificiales, galerías de minas y otras oquedades deberán ser basados en métodos directos de observaciones y mediciones en las cavidades o en sondeos.

e) Los métodos indirectos, incluyendo los geofísicos, solamente se emplearán como apoyo de las investigaciones directas.

f) Los sondeos a realizar podrán ser de los siguientes tipos indicados a continuación, se describen de manera específica en el Apéndice 1 “Postes” del Anexo Técnico en su Capítulo 2.

- Sondeos con recuperación continúa de muestras alteradas mediante la herramienta de penetración estándar.
- Sondeos mixtos con recuperación alternada de muestras inalteradas y alteradas.
- Sondeos consistentes en realizar, en forma continua o selectiva, una determinada prueba de campo.
- Sondeos con equipo rotatorio y muestreadores de barril.
- Sondeos de percusión o de avance con equipo tricónico o sondeos con variables de perforación controladas.
- Sondeos tipo STP con profundidad de 3.5 metros, con lectura del número de golpes de acuerdo a la norma ASTM-D- 1586.

g) Se deberán de realizar los Ensayes de laboratorio Geotécnico a las muestras tomadas, para determinar las propiedades índice.

h) Con los datos obtenidos de laboratorio se determinara la capacidad de carga y resistencia de suelo.

Se deberá de realizar el levantamiento de la estratigrafía de los mantos que se localicen, presentando su profundidad con respecto a cada estrato con el objeto de clasificar el tipo de suelo de acuerdo al SUCS (Ver Apéndice 1 “Postes” del Anexo Técnico en su Capítulo 2).

Especificaciones para el Diseño de Cimentación.

Los postes son estructuras ligeras con excavaciones someras que deben de cumplir con los siguientes parámetros para cada tipo de suelo de acuerdo a la clasificación de las zonas (Ver Apéndice 1 “Postes” del Anexo Técnico en su Capítulo 2).

1. Peso unitario medio de la estructura $w \leq 40$ kPa (4 t/m²).
2. Perímetro de la construcción:
    a. $P \leq 80$ m en las zonas I y II; o
    b. $P \leq 120$ m en la zona III.

Profundidad de desplante $D_f \leq 2.5$ m.

a) En los suelos de lomas si se considera en el diseño del cimiento un incremento neto de presión mayor de 80 kPa (8 t/m²), el valor recomendado deberá justificarse a partir de los resultados de las pruebas de laboratorio o de campo realizadas.

b) En los suelos de transición si se considera en el diseño del cimiento un incremento neto de presión mayor de 50 kPa (5 t/m²), el valor

recomendado deberá justificarse a partir de los resultados de las pruebas de laboratorio o de campo realizadas.

c) En los suelos lacustres si se considera en el diseño del cimiento un incremento neto de presión mayor de 40 kPa (4 t/m²), el valor recomendado deberá justificarse a partir de los resultados de las pruebas de laboratorio o de campo realizadas.

d) En el diseño de la cimentación del poste, se deben considerar los siguientes estados límite de falla de la estructura, además de los correspondientes a los miembros de la misma:

1. Flotación;
2. Flujo plástico local o general del suelo bajo la cimentación; y
3. Falla estructural de pilotes, pilas u otros elementos de la cimentación.

Las combinación de acciones a considerar en el diseño de las cimentaciones (Ver Apéndice 1 “Postes” del Anexo Técnico en su Capítulo 2), deberán ser las siguientes:

1. Primer tipo de combinación. Acciones permanentes más acciones variables.
2. Segundo tipo de combinación. Acciones permanentes más acciones variables con intensidad instantánea y acciones accidentales (viento o sismo).

Especificaciones del Cimiento del Poste.

Con base en los resultados del análisis de los estudios de geotecnia, geofísico y mecánica de suelos, de donde se instalaran los postes, se podrá determinar las dimensiones y profundidad de desplante del cimiento, el cual deberá de cumplir con las siguientes especificaciones técnicas:

a) La cimentación debe de ser un micro pilote de sección uniforme de concreto armado con acero de refuerzo convencional.
b) El concreto debe ser estructural Clase I.
c) Resistencia mínima del concreto a la compresión será de f´c = 250 Kg/cm^2.
d) El módulo de elasticidad del concreto debe ser Ec = 221,300 Kg/cm^2.
e) El acero de refuerzo deberá de tener una fluencia de fy=4200 Kg/cm^2.
f) Resistencia del acero de refuerzo de Es = 2, 039, 000 Kg/cm^2.
g) La construcción del cimiento deberá de tener como armado 6 varillas del número 6 y estribos del número 2.5 a cada 20cm de distancia de separación.
h) Instalación y construcción del Cimiento del poste en sitio.- Se deberá de excavar y construir a una profundidad de desplante igual a la altura de diseño del cimiento más 30cm, y con un ancho de excavación igual al del cimiento más el 100%, de tal forma que permita las actividades de construcción como son la colocación de plantilla, armado de acero, cimbrado y colado del mismo, con el objeto de que este sea estable ante la acción de las cargas permanentes y accidentales como viento y sismo.
i) Instalación del Cimiento prefabricado del poste.- Se deberá de excavar e hincar a una profundidad de desplante igual a la altura de diseño del cimiento más 30cm, y con un ancho de excavación igual al del cimiento más el 50%, de tal forma que permita las maniobras de colocación como son la plantilla y fijación del perímetro del cimiento al suelo existente con lodo bentonítico, con el objeto de que este sea estable ante la acción de las cargas permanentes y accidentales como viento y sismo.

IV.2.3.2 Especificaciones Técnicas para el Diseño del Poste.

Exploración Geográfica y Estudio de Velocidades del Viento.

a) Se deberán de determinar los factores topográficas y de exposición locales donde se desplantará la construcción del cimiento de acuerdo a la clasificación del terreno, que está en función del grado de rugosidad (Ver documento Apéndice 1 “Postes” del Anexo Técnico en su Capítulo 2).
b) La categoría para cada tipo de terreno, está asociada con velocidades de ráfagas de 3 segundos y evaluadas a 10 m de altura en terreno plano.

c) Los periodos de retorno de 10, 50 y 200 años están en función de los mapas isotacas.

Parámetros de Diseño del Poste.

a) Para el diseño por sismo se debe de considerar la zona sísmica**.**
b) El poste se considera del grupo “B” de acuerdo a su grado de seguridad, cuyo coeficiente será (C=0.45*1.5=0.675).
c) Factor de reducción Q=5.
d) Para el Diseño del poste por Viento, la estructura de acuerdo a su importancia se clasifica como del Grupo “B”.
e) Clasificación de la estructura de acuerdo a la respuesta ante la acción del viento es del Grupo “3”.
f) Periodo de retorno de la velocidad del viento será de 200 años.
g) Velocidad regional del viento para estados del centro de la republica V_R = 90 m/s.
h) Velocidad regional del viento para estados del norte de la republica V_R = 125 m/s.
i) Velocidad regional del viento para estados de costa de la republica V_R = 170 m/s.
j) Las estructuras deberán de tener una vida útil de 50 años como mínimo.
k) Las acciones del viento que deben considerarse para el diseño del poste son la acción número III.
l) La densidad del aire se deberá tomar igual a 1.225 kg/m^3.

Propiedades Geométricas.

a) El poste deberá de actuar como un sistema estructural en voladizo cuya sección transversal deberá de ser continua, desde la placa base hasta la punta el mismo.

b) El poste de acero deberá de estar hecho con una placa de espesor de 0.1875 de pulgada (3/16”), en toda su altura.

c) El poste deberá de contar con soportes para Gabinete de equipos, soporte para cámara, soporte de sensor de disparo y en su caso si lo requiere, soporte de extensión para brazo con cámara.

d) El poste, herrajes y accesorios deberán de contar con protección ante el intemperie, por medio de la aplicación del galvanizado por inmersión en caliente, cuyo espesor deberá de ser como mínimo 4.3 mls de acuerdo a ASTM A-123.

e) El acero del poste deberá de ser del tipo estructural (ASTM A-36) con un fy = 2530 Kg/cm^2, Es = 2, 039, 000 Kg/cm^2.

f) El brazo del poste deberá de ser de tubo de 2 ½ pulgadas de radio, con cedula 40, que servirá para alojar la cámara y en su caso sensor de disparo.

g) Los Herrajes del poste deberán de tener una cedula de 40.

h) La tornillería y tuercas del poste deberán de ser de acero estructural de alta resistencia ASTM A-325.

A continuación se presentan varias figuras que describen de manera general la cimentación, plantas de cimentación, anclajes de cimentación, la base y alzado con geometría de los postes. Con intención de ilustrar lo antes escrito en este capítulo.

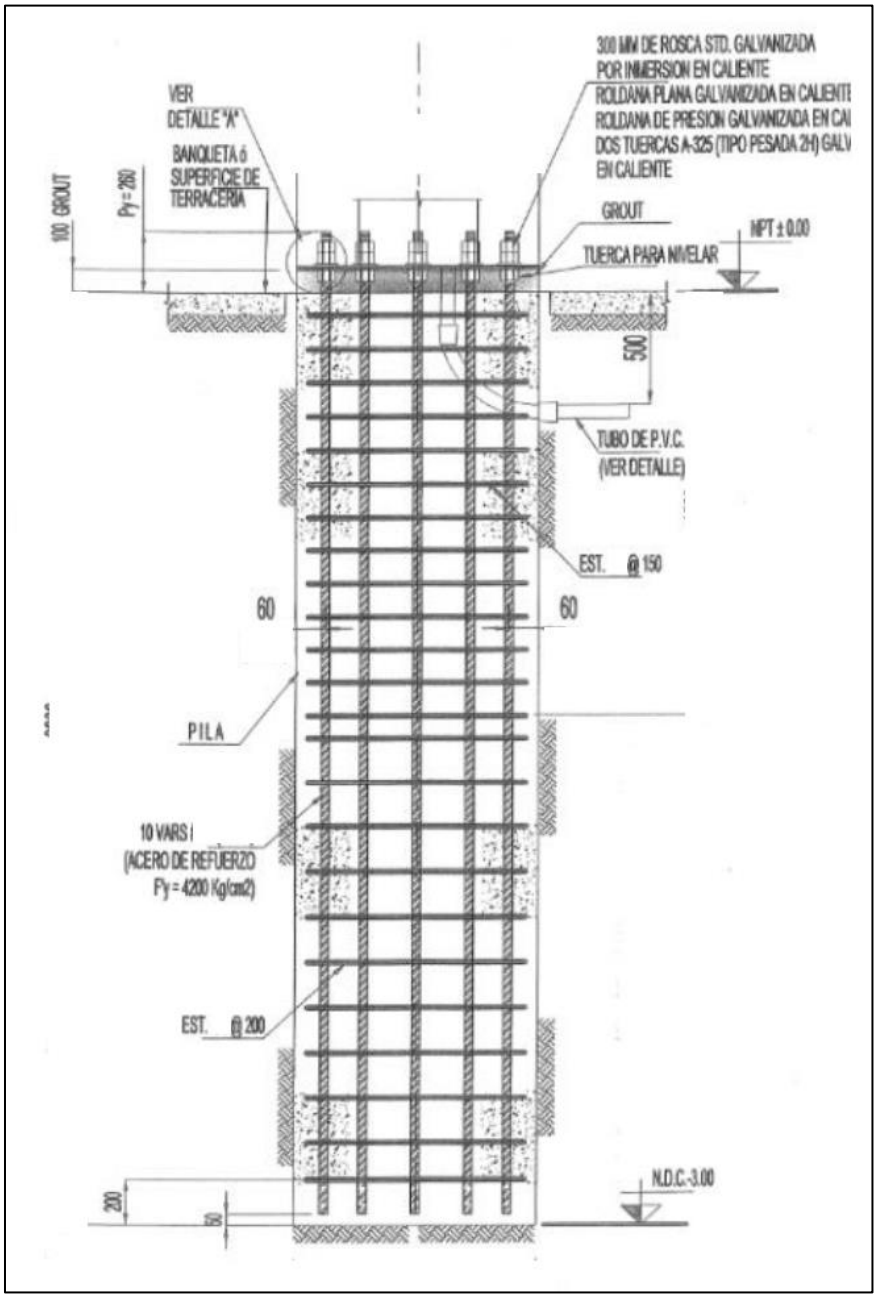


Figura IV.2.1 Cimentación poste de 12 a 20 metros

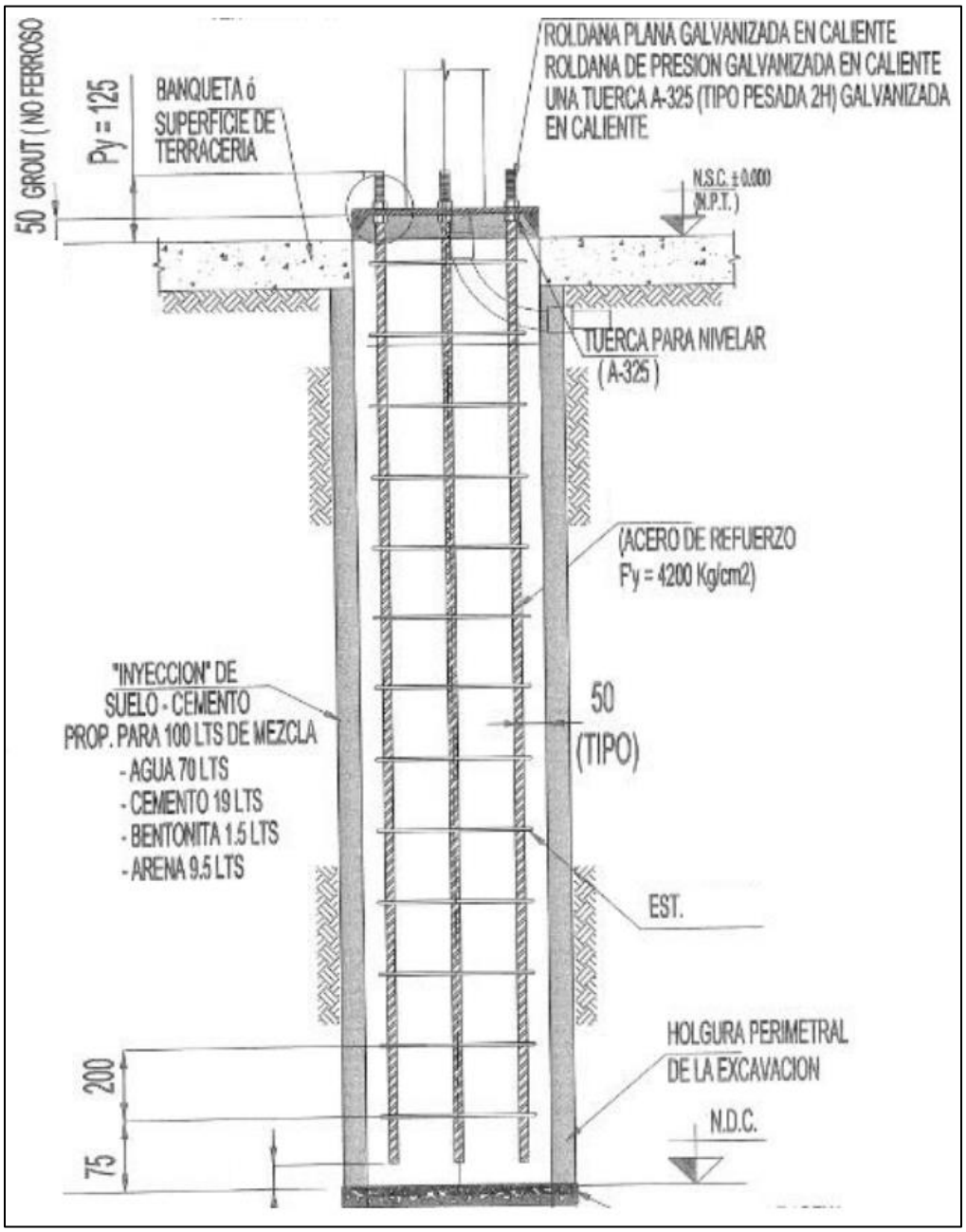


Figura IV.2.2 Cimentación poste de 9 a 11 metros de altura

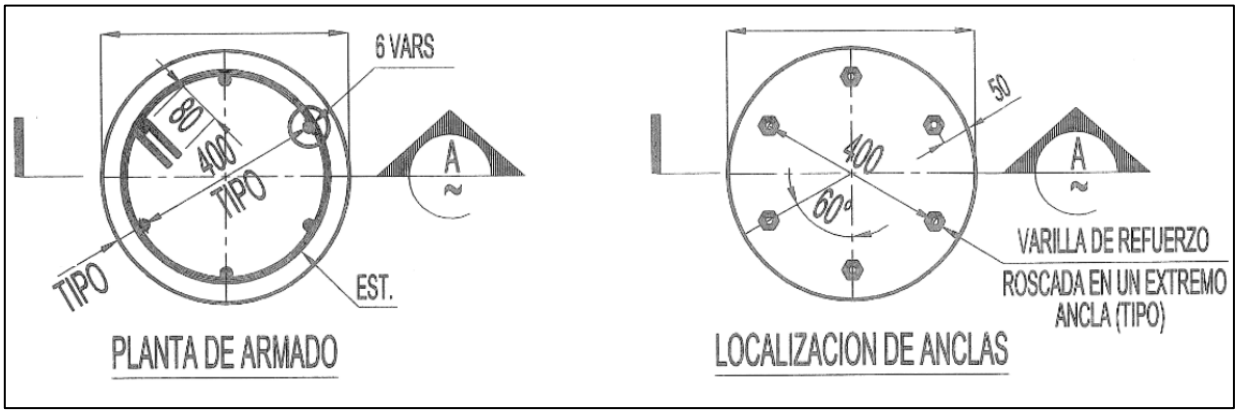


Figura IV.2.3 Planta de Cimentación y Anclas de poste de 9 a 11 metros

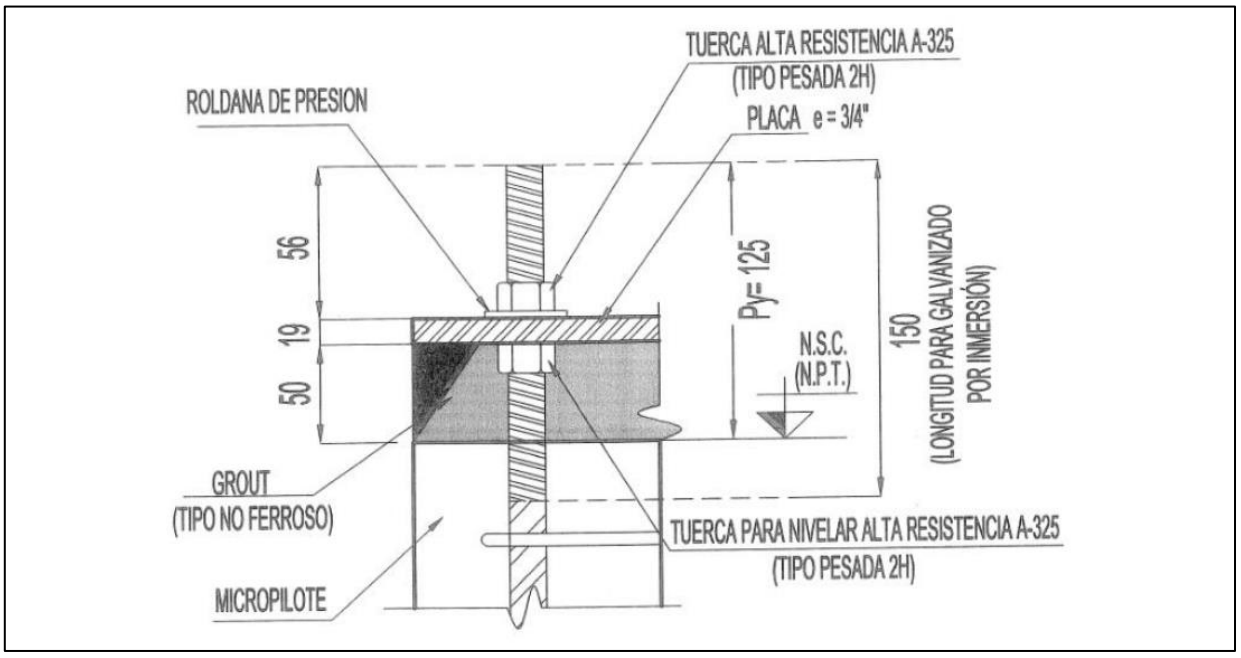


Figura IV.2.4 Detalle "A" de Anclaje de Cimentación de poste de 9 a 11 metros

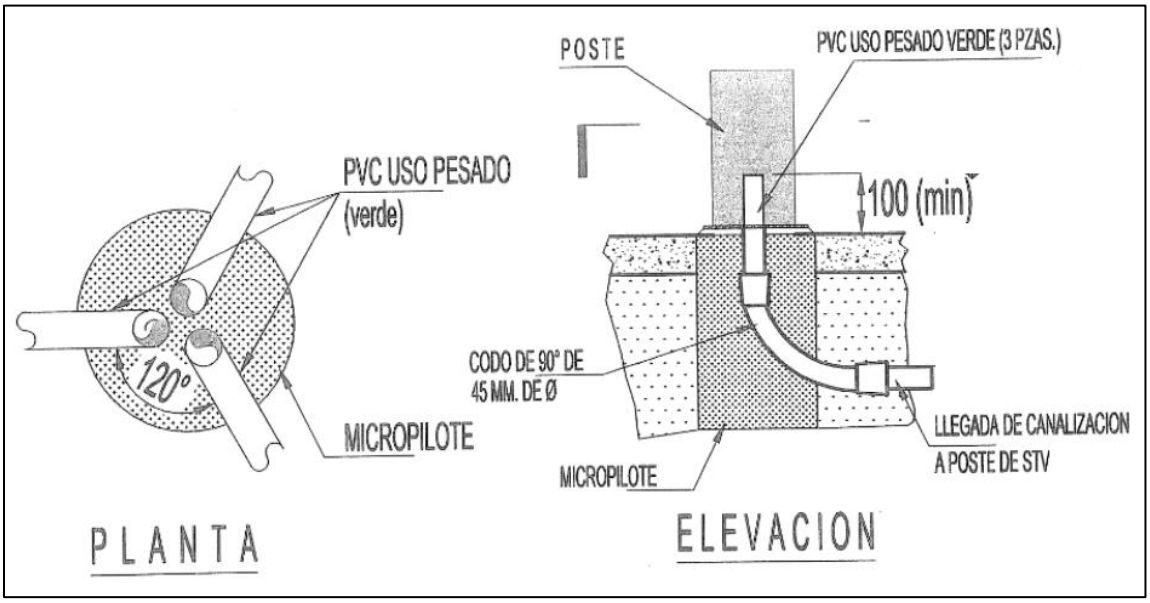


Figura IV.2.5 Detalle de Acometida al poste de 9 a 11 metros

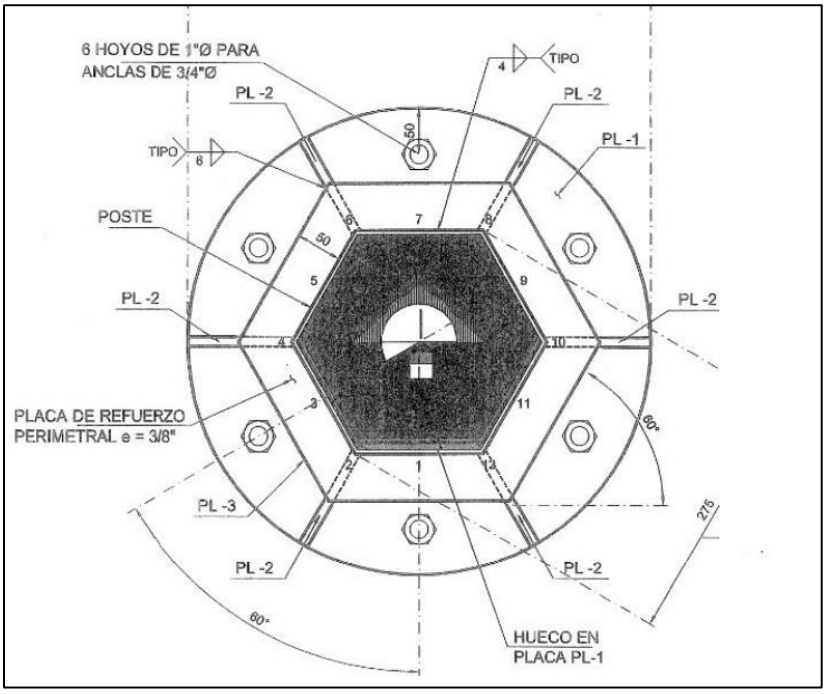


Figura IV.2.6 Base Metálica de poste de 9 a 11 metros

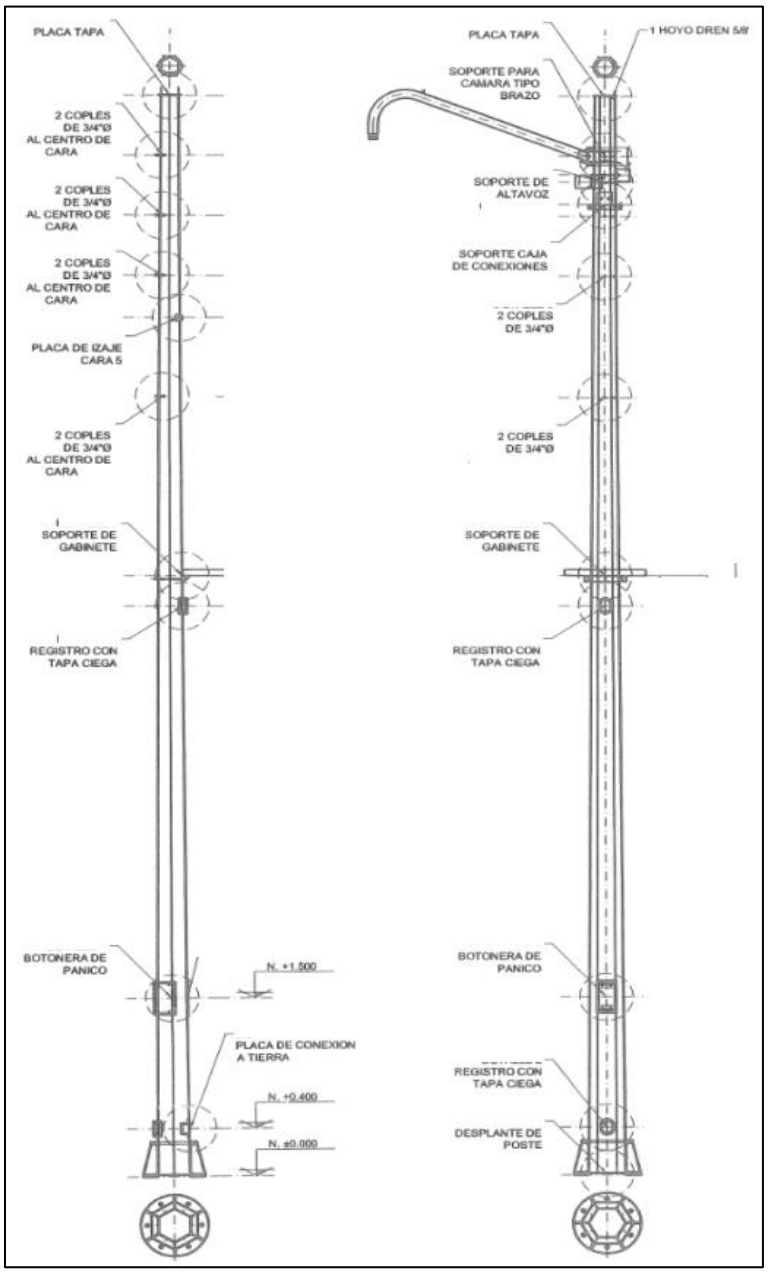


Figura IV.2.7 Alzado de poste con geometría

Una vez que se han establecido los criterios normativos relativos a la cimentación y diseño de postes, en el siguiente capítulo se abordará todo lo relativo al punto de monitoreo inteligente.

IV.3 Punto de Monitoreo Inteligente.

IV.3.1 Justificación.

El Punto de Monitoreo Inteligente (PMI) es la base del sistema de video vigilancia. Es el mecanismo a través del cual se adquieren los datos e imágenes que permiten realizar las acciones correspondientes ante cualquier eventualidad, a partir del monitoreo en el centro de control. De forma general, un PMI se compone de los dispositivos mostrados en la figura IV.3.1

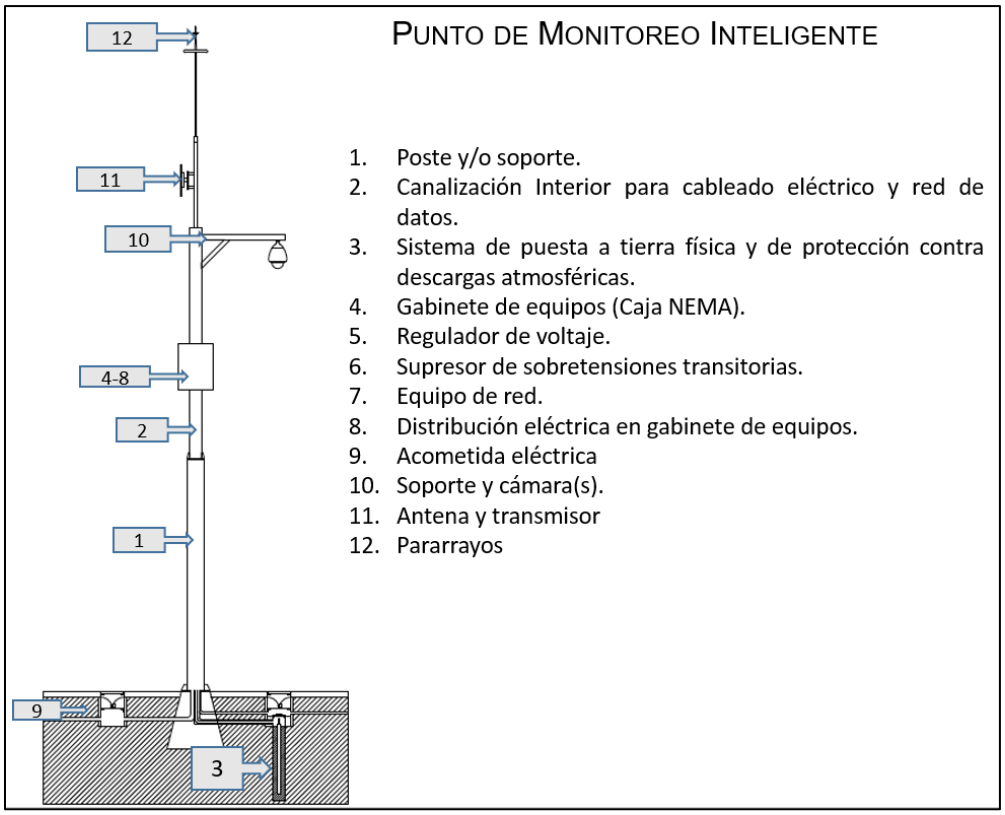


Figura IV.3.1 Punto de Monitoreo Inteligente

Una parte fundamental en el PMI es la cámara de video. Esta debe obtener imágenes de manera clara y con el mayor detalle posible, de manera que el individuo que ha cometido un delito pueda ser detectado y reconocido por la red de cámaras del SVV. Esta facultad permite que, durante la investigación de un crimen, las autoridades tengan la posibilidad de generar mayor evidencia sobre el sujeto o sujetos imputados.

Por lo tanto, la cámara debe tener la suficiente potencia para captar y transmitir las imágenes en una alta calidad. De acuerdo con el análisis incluido en el Anexo Técnico, una cámara de 1.3 MPx de lente varifocal es el estándar para obtener el suficiente detalle de una escena. Así mismo, se propone la adopción de la tecnología de compresión de video H.265, la cual permite reducir el ancho de banda sin sacrificar la calidad del video.

Esta Norma propone que se utilice como estándar una cámara tipo Domo PTZ y/o PTZ por dos razones principales: 1) las cámaras PTZ cuentan con un movimiento horizontal de prácticamente 360º y de 180º en vertical, mientras que las cámaras fijas (como las que se usan en monitoreo de tráfico) no permite hacer paneos, por lo que cuentan con múltiples puntos ciegos; y 2) el uso del domo permite ocultar la dirección de apuntamiento del lente, además de proteger a la cámara de posibles actos vandálicos.

No se debe pasar por alto que la Norma busca promover la interoperabilidad de los SVV para incrementar la eficacia en la estrategia de seguridad pública. La adopción de estándares tecnológicos, como las cámaras de video propuestas en este documento o los protocolos de compresión, orientan a las entidades federativas a hacer una inversión inteligente de los recursos.

IV.3.2 Glosario.

Para contextualizar la información en el ámbito de la presente Norma, se presenta a continuación un glosario de términos y definiciones relacionadas.

- Alarma: Capacidad de respuesta del componente del sistema de video-vigilancia a un impulso o señal externa de alarma, se usa para iniciar funciones pre-programadas en dispositivos como por ejemplo la activación de movimiento de un Domo PTZ hacia una determinada ubicación.
- Análisis de vídeo (Analytics): Esta tecnología se emplea en los sistemas de video-vigilancia para detectar de forma automática a personas y vehículos en situaciones no comunes (sospechosas) dentro de la escena inspeccionada, lanzando diversas alarmas, definidas por el sitio de monitoreo.
- Angulo de visión: Área de imagen de una cámara, dependiendo de la lente instalada.

- Auto-Iris: Control de apertura de la lente para una mejor calidad de video bajo diversas y cambiantes condiciones lumínicas.
- Cámaras de alta definición: Este tipo de cámaras ofrece resoluciones superiores a las obtenidas con cámaras analógicas
- Cámaras Día/Noche: Las cámaras de seguridad que tienen esta especificación poseen una sensibilidad a la luz de por lo menos 0.01 lux lo que las hace efectivas para monitoreo en lugares con muy poca luz. En estas condiciones, estas cámaras cambian su configuración de color a blanco y negro automáticamente, logrando una sensibilidad a la luz mucho mayor.
- Cámaras PTZ (Pan-Tilt-Zoom): En estas cámaras se encuentran instalados motores que permiten el control remoto para el apuntamiento de la cámara tanto vertical (elevación) como horizontalmente (azimut), esta característica permite lograr la inspección de una zona en 360°, también cuentan con la capacidad de realizar acercamientos (zoom) para obtener detalles de algún punto de interés.
- Cámaras IP: Mediante las cámaras IP se obtienen mayores resoluciones que con cámaras analógicas convencionales. Por otro lado el ancho de banda utilizado es menor debido a la compresión de video, también permiten realizar el monitoreo, no solo del video transmitido, sino que también permiten conocer su estado.
- Cámaras para el reconocimiento de matrículas (LPR): Son empleadas regularmente para control de tráfico y deben ser colocadas de tal manera que permitan obtener imágenes claras de las matrículas de los automóviles para su detección y reconocimiento.
- CCD (Charge-Coupled Device): Es un sensor para la captura de imágenes compuesto por un circuito integrado y un arreglo de capacitores.
- CCTV: Circuito Cerrado de Televisión. Es un Sistema de Vigilancia Utilizado para ver imágenes / videos en privado y no para uso público.
- CIF (Common Intermediate Format): Se refiere al tamaño o resolución de una imagen en el ámbito analógico.
- CMOS (Complementary Metal Oxide Semiconductor): Dispositivo de conmutación de estado sólido. Es un tipo de Sensor de imagen de video de las cámaras.

- Compresión: Métodos que permiten disminuir el tamaño inicial de una imagen digitalizada aplicando algoritmos que eliminan información redundante a expensas de la calidad de la imagen final.
- Descompresión: Transformar la información comprimida digitalmente y reproducir las imágenes de video normal.
- Definición de la cámara: Capacidad de una cámara o monitor de reproducir fielmente las imágenes capturadas.
- Distancia focal: Distancia medida en milímetros entre la lente y el sensor que determina el ángulo de visión que se obtiene.
- Escaneo Entrelazado: Consiste en la transmisión de un primer campo compuesto por las líneas impares de la imagen y a continuación un segundo campo formado por las líneas pares.
- Escaneado progresivo: El escaneado progresivo, a diferencia del entrelazado, escanea la imagen entera, línea a línea, cada 1/16 segundos. En otras palabras, las imágenes captadas no se dividen en campos separados como ocurre en el escaneado entrelazado, de forma que prácticamente no existe ningún efecto de parpadeo. En una aplicación de vigilancia esto puede resultar vital para ver los detalles de una imagen en movimiento, como una persona que está corriendo.
- Grabador de video digital DVR: Almacena las imágenes tomadas de canales distintos de grabación. En algunos casos cuentan con detectores de movimiento, entradas de alarma y sistema de conexión remota.
- Infrarrojo (IR): Las cámaras de seguridad que poseen esta funcionalidad pueden captar imágenes aun en oscuridad absoluta dentro de cierto rango de distancia que depende del número y tipo de leds que contengan. Comúnmente tienen entre 8 y 60 leds.
- Iluminación: Cantidad de luz de una escena concreta por metro cuadrado, la unidad de medida es el LUX.
- Iris: Mecanismo interno del lente para regular la cantidad de luz que pasa a través de él y llega al sensor CCD.
- Iris automático (o iris de tipo DC): Este tipo especial de iris está controlado eléctricamente por la cámara, para regular automáticamente la cantidad de luz que se permite entrar.

- Isoceráunico: Número promedio de días al año en los que hay tormenta en una región.
- Lux: Unidad de medida de intensidad de luz. Se usa para medir el nivel de luz mínimo al cual una cámara de seguridad puede captar imágenes de manera satisfactoria.
- Megapíxel: Un megapíxel es una unidad que equivale a 1 millón de píxeles (px). Esta unidad se usa para expresar la resolución de imágenes digitales. MPEG-4: Es un grupo de estándares de codificación de audio y vídeo.
- NTSC (National Television System Committee): Es un sistema de codificación y transmisión de televisión analógica empleado en América y Japón. Su especificación es 525 líneas a 60Hz.
- PAL (Phase-Alternating Line): Es el sistema de codificación y transmisión de televisión analógica, es empleado en diversos países africanos, asiáticos, europeos, algunos países americanos y Australia. Su especificación es 625 líneas a 50Hz.
- Pixel: Es la unidad usada para expresar la resolución.
- Profundidad de campo: Es el área bajo inspección enfocada por una cámara dentro de la cual la imagen obtenida es nítida. La profundidad de campo aumenta al emplear el zoom.
- PoE (Power over Ethernet): Es una tecnología que permite a los equipos en red obtener la alimentación mediante el cable Ethernet.
- Protocolo: Lenguaje de comunicación estandarizado para diferentes dispositivos
- Resolución: Es una medida del grado de detalle de una imagen digital, se puede especificar como el número de columnas de píxeles (horizontal) por el número de filas de píxeles (vertical).
- Sensibilidad: Se refiere a la luminosidad necesaria para obtener una imagen de video con calidad estándar, su unidad de medida es el lux.
- Trama (Frame): Se refiere al número de cuadros por segundo (fps) al cual se muestra o graba el video. Las transmisiones de TV convencionales son a 30 fps, ya que esta tasa es considerada como video en tiempo real.
- Sistema de alimentación ininterrumpida (UPS): es un dispositivo que cuenta con baterías capaces de almacenar energía eléctrica para proporcionar alimentación a los equipos conectados a éste durante un corte de energía eléctrica de la red pública.

- Varifocal: Este es un tipo de lente que permite el ajuste de la distancia entre dos puntos focales para obtener tomas más cercanas o lejanas del escena bajo inspección (permite aplicar zoom).
- Zoom: El zoom se encuentra ligado al lente de la cámara, esta característica permite acercar la toma para obtener mayores detalles de un objeto específico en la escena bajo inspección.

IV.3.3 Lineamientos normativos.

IV.3.3.1 Características Mínimas de la Cámara.

Video.

a) La cámara deberá emplear la tecnología Digital IP.

b) La resolución mínima con la que debe contar la cámara debe ser 1.3 MP.

c) El lente debe ser Varifocal: 4.3 mm a 129 mm. F1.6 (hasta el cierre) a F4.7 (hasta el cierre).

d) El sensor a emplear deberá ser preferentemente CCD 1/3'' o CMOS opcional.

e) El zoom con el que debe contar la cámara debe ser de al menos 30X óptico (4.3 mm).

f) La cámara deberá trabajar a 30 fps.

g) La compresión con la que deberá trabajar la cámara es H.265.

h) La cámara empleada deberá permitir realizar ajuste de imagen en color, brillo, nitidez, balance de blancos, control de exposición y compensación de contraluz (auto-iris).

i) La cámara debe contar con tecnología Día/Noche.

j) Video inteligente: detección de movimiento por video que será opcional dependiendo de las necesidades de cada sistema.

k) Activador de alarma que será alertado por video inteligente (opcional).

Nivel de Red.

a) La cámara IP seleccionada debe ser compatible con diferentes protocolos de comunicación actuales: RIPv2/OSPF, IPv4/v6, HTTPS, QoS DSCP, FTP, TFTP, SNMP v2c/v3, SNTP, IGMP, DHCP, SSHv2, PIM-SM, DVMRP, Syslog, RMON.
b) La seguridad deberá permitir uso de contraseña, filtro de dirección IP, cifrado HTTPS, control de acceso a red IEEE 802.1x.
c) Para permitir la escalabilidad la cámara deberá ser un Sistema abierto a carga de nuevas versiones, carga de archivos por medio de FTP y correo electrónico.

Nivel Físico.

a) El tipo de cámara a emplear por los SVV del país debe ser tipo domo PTZ y/o PTZ.
b) Al ser una cámara PTZ debe permitir el movimiento horizontal de 360° y vertical de 0° a 90°.
c) La protección de la cámara contra vandalismo y aspectos climatológicos debe ser IP66.
d) La cámara deberá contar con el herraje apropiado para su montaje.
e) El peso de la cámara instalada deberá ser menor a 10 Kg.
f) El intervalo de temperatura que deberá soportar la cámara debe encontrarse entre –35°C a 60°C.
g) La conexión de entrada de la cámara debe ser compatible con los conectores RJ-45 10BASE-T/100BASE-TX.
h) La alimentación debe ser compatible con PoE+.
i) La memoria extraíble en las cámaras para guardar video localmente es opcional.

IV.3.3.2 Características del Altavoz.

Audio.

a) Las compresiones de audio con la que deberá poder trabajar el altavoz son G.711, G.722, G.726.
b) El altavoz debe emplear tecnología IP.
c) El altavoz debe tener una potencia mínima promedio de 15 Watts.
d) El nivel de presión sonora mínimo manejado por el altavoz debe ser de 106 dB.

e) El altavoz debe tener un rango de respuesta en frecuencia de 330 Hz a 8000 Hz.

f) La impedancia del altavoz debe ser de 8 Ω.

Nivel de Red.

a) El altavoz IP debe ser compatible con los diferentes protocolos de comunicación actuales: RIPv2/OSPF, IPv4/v6, HTTPS, QoS DSCP, FTP, TFTP, SNMP v2c/v3, SNTP, IGMP, DHCP, SSHv2, PIM-SM, DVMRP, Syslog, RMON.

b) La seguridad del altavoz debe tener Protección por contraseña, filtro de direcciones IP, registro de acceso de usuarios, autenticación.

c) La conexión de entrada al altavoz debe ser compatible con los conectores RJ-45

d) La administración y operación deberán ser HTTPS (configuración Web), DHCP, IP, actualización y configuración remota, monitoreo centralizado.

Nivel Físico.

a) El altavoz deberá tener protección y resistencia a impactos cumpliendo con los protocolos Polvo y agua, IP66, IP67, NEMA.

b) La alimentación debe ser Ethernet (PoE+)

c) El altavoz debe tener la capacidad de trabajar en condiciones climáticas de -35°C a 60°C Humedad Relativa < 95%.

d) El peso del altavoz deberá ser menor a 5 Kg.

IV.3.3.3 Características del Sistema de Protección contra Descargas Eléctricas.

a) Según la norma NMX-J-549-ANCE-2005, el pararrayos deberá ofrecer un punto de impacto al rayo con condiciones controladas, en una trayectoria de baja impedancia menor a 10Ω disipándose por medio de los elementos del sistema de puesta a tierra.

b) Por lo tanto el PMI deberá contar con un sistema de pararrayos, previniendo riesgos por descargas atmosféricas de acuerdo a las normas oficiales mexicanas NOM-001-SEDE-2012 Y NOM-022-STPS-1999. Para la instalación del o los para-rayos debe ser considerado:

i. El nivel isoceráunico de la región.
ii. Las características físicas de las estructuras e instalaciones metálicas que soportan descargas eléctricas atmosféricas.
iii. La altura de los edificios colindantes.
iv. Las características y resistividad del terreno.
v. El ángulo o zona de protección del pararrayos.
vi. La altura del pararrayos y el sistema para drenar a tierra las corrientes generadas por las descargas eléctricas atmosféricas, en este sentido la norma NMX-J-549-ANCE-2005 propone emplear terminales aéreas con una altura recomendable de 3 metros por encima del objeto a proteger.
vii. La resistencia de la red de tierras para colocar los sistemas de pararrayos no debe ser en ningún caso mayor a 10Ω. Los conductores de bajada en cobre se presentan bajo la forma de cintas, trenza, o redondos de sección mínima 1/0AWG ($50mm^2$).
viii. Que no se deben utilizar pararrayos que funcionen a base de materiales radiactivos.
ix. La Instalación de una funda de protección mecánica de 2m al final del cable bajante.
x. Que las masas metálicas exteriores deben estar conectadas equipotencialmente al circuito de pararrayos según las normas de distancia de seguridad de la NFC 17-100 que describe también las distancias a respetar entre las bajadas.
xi. Que cuando hay una antena de radio, y en conformidad a la norma NFC 90-120, se debe conectar el mástil que soporta la antena, al conductor de bajada de la instalación, por intermedio de un supresor de transitorios o de un metal común.
xii. Que ciertos elementos metálicos de la estructura pueden servir para realizar la bajada si cumplen con los criterios de las normas NF C 17-100 y NF C 17-102.

IV.3.3.4 Sistema de Tierra.

a) El sistema de tierra deberá garantizar una resistencia a tierra no mayor de 10Ω.

b) El sistema de tierra estará conformado por varillas de tierra, conectores para varilla de tierra y materiales para el reacondicionamiento del terreno en caso necesario.

c) Para la instalación del sistema de tierra deberá realizarse el estudio en sitio con el cual se propondrá la configuración requerida para garantizar los 10Ω como máximo de resistencia a tierra en época de sequía.

Deberán conectarse en el subsuelo la bajante del sistema de pararrayos, el sistema de tierras del sistema eléctrico y la estructura metálica para garantizar que los equipos y las masas metálicas se encuentren a un mismo potencial de referencia con conectores soldables, como mínimo este conductor deberá ser de 4/0AWG (107 mm^2).

IV.3.3.5 Características del Sistema de Alimentación (UPS).

a) El UPS deberá tener la capacidad de cubrir las necesidades del PMI.
b) Este se conectará a un contacto dúplex polarizado con alimentación a 127 VCA, 60 Hz y salida regulada a 127 volts.
c) El UPS dará alimentación a todos los equipos en el PMI (cámaras, altavoces, intercomunicadores o botones de pánico y equipos de comunicación).
d) Las características principales con las que deberá contar se enlistan a continuación:
    i. Un tiempo de respaldo de por lo menos 30 min.
    ii. Operación automática con supresión de picos transitorios y armónicos.
    iii. Contar con puertos de comunicación para conexión a la Red para su monitoreo en tiempo real.
    iv. Debe contar con un sistema de tierra física observando la NOM-001 SEDE 2012 referente a instalaciones eléctricas.
    v. Contar con un sistema de protección contra descargas eléctricas atmosféricas (pararrayos) que proteja contra este tipo de eventualidades.

e) El UPS debe estar protegido por una caja NEMA instalada a 5 metros de altura sobre la base del poste con un nivel de protección 4X, equivalente al IP66.

Para detalles de la selección y características del UPS, por ejemplo potencia, ver anexo técnico en el apartado 3.4.4.

Se ha revisado con gran detalle cada uno de los elementos de un Punto de Monitoreo Inteligente, de manera lógica nuestro apartado siguiente versará sobre las telecomunicaciones, mismas que se encargaran de comunicar a las cámaras con el centro de control.

IV.4 Telecomunicaciones.

IV.4.1 Justificación.

Como se mencionó al inicio de este documento, el sistema de comunicaciones es una de las partes más importantes en un SVV, ya que es el responsable de enlazar a los Puntos de Monitoreo Inteligente (PMI) con el Centro de Control. Si esta comunicación es ineficiente, de poco sirve que la captura de imágenes sea en alta calidad o que el Centro de Control cuente con tecnología de punta.

Con base en la información encontrada en las visitas a los SVV de diferentes Centros de Control, se presentan los dos puntos más relevantes que se deben atender en el diseño de los nuevos sistemas de video vigilancia: 1) el equipamiento del sistema; y 2) la administración del sistema.

Sobre el equipamiento, se detectó que la mayoría de los equipos encontrados en los SVV pertenecen a una sola marca. Esto, lejos de generar un estándar, deriva en un monopolio. Por esa razón, las especificaciones técnicas indicadas en este documento promueven el uso de protocolos de comunicación abiertos, de modo que se garanticen las buenas prácticas y exista una mayor apertura del mercado a diversos fabricantes.

Asimismo, la administración, control y mantenimiento de los SVV son realizados mayormente por el proveedor que implementó el sistema. Si bien el proveedor cuenta con el personal adecuado para brindar soporte técnico, mantenimiento y corrección de fallas, esta situación genera una dependencia del usuario hacia el tiempo de respuesta del proveedor para atender cualquier falla. El efecto de esta práctica también apunta hacia el monopolio, ya que el único proveedor puede encarecer arbitrariamente los servicios al no contar con competidor alguno. Esto, por supuesto, en detrimento del gasto eficiente de los recursos.

Otro problema identificado es que los proveedores no proporcionan documentación al usuario del SVV, lo que dificulta la autogestión o la de entrada de otros proveedores. Para solucionar eso, la Norma establece que el proveedor debe dotar –antes, durante y

después de la implementación– el diseño del proyecto, los protocolos de prueba, las pruebas de aceptación al sistema, las memorias técnicas, la capacitación al personal, los programas de mantenimiento y el protocolo de atención al cliente.

Este apartado también contempla los requisitos generales previos a cubrir para la selección del equipo, los protocolos de comunicación y demás parámetros. Todas esta información específica puede consultarse en el Anexo Técnico.

De igual manera, la Norma presenta la normatividad aplicada y las condiciones sobres diversos enlaces entre el PMI y el Centro de Control, así como los protocolos, estándares y recomendaciones de la Unión Internacional de Telecomunicaciones (UIT, por sus siglas en inglés), del Instituto de Ingeniería Eléctrica y Electrónica (IEEE, por sus siglas en inglés) y la Fuerza de Trabajo de Ingenieros de Internet (IETF, por sus siglas en inglés), perteneciente al Comité de Arquitectura de Internet (IAB, por sus siglas en inglés).

IV.4.2 Glosario.

Para contextualizar la información en el ámbito de la presente Norma, se presenta a continuación un glosario de términos y definiciones relacionadas.

- Ancho de Banda: Valor de la diferencia entre dos frecuencias límite de una banda de frecuencias.
- ADSL: Asymmetrical Digital Subscriber Line. Línea Digital Asimétrica de Usuario. Tecnología modem que proporciona mayor ancho de banda que las líneas telefónicas de última milla ordinarias. Lo asimétrico es capaz de proporcionar una conexión más rápida entre la oficina central y el local del cliente.
- AES: Advanced Encryption Standard. Norma de encriptación avanzada.
- ATU-C: ADSL Terminal Unit-Central. Unidad de terminación ADSL-Centro (oficina).
- ATU-R: ADSL Terminal Unit-Remote. Unidad de terminación ADSL-Remota.
- Banda de frecuencias: Conjunto continuo de frecuencias comprendidas entre dos frecuencias límite especificadas
- BPSK: Binary Phase-Shift Keying. Modulación por desplazamiento de fase binario.

- Calidad de servicio (QoS): La totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas de un servicio de usuario.
- Conmutador de datos (switch): Equipo de comunicaciones de capa 2 del modelo OSI, su función es reenviar tramas que llegan por sus puertos a otro puerto para que alcance su destino.
- Corta Fuego: Sistema o combinación de sistemas que establecen una frontera de seguridad entre dos o más redes, su función es restringir el tráfico de datos que pasa de una red a otra.
- DBA: Dinamic band with alocation. Asignación dinámica de ancho de banda opera en la OLT.
- DES: Data Encryption Standard. Norma de encriptación de datos.
- DHCP: Protocolo de configuración dinámica del host. permite que el host obtenga la dirección IP de forma dinámica sin que el administrador de red tenga que configurar un perfil individual para cada dispositivo.
- DSCP: Differentiated Services Code Point. Es un método para marcar paquetes IP para darles diferentes prioridades. La marca se pone en el campo TOS del encabezado IP.
- DSL: Digital Subscriber Line. Línea de suscriptor digital. Es el nombre génerico que identifica las tecnologías ADSL, HDSL, VDSL, etc, todas son tecnologías de la última milla.
- DSLAM: Digital Subscriber Line Access Multiplexor. Multiplexor de acceso de abonado digital. Es el equipo que conecta la red de transporte con la red de acceso o la red de acceso con la red el abonado en una tecnología DSL.
- DVMRP: Distance Vector Multicast Routing Protocol. Protocolo de enrutamiento demultidifusión de vectores de distancia.
- E1: Enlace de transmisión digital con una relación total de transmisión y recepción de 2.048 Mbps.
- Enrutador: Aparato que reenvía segmentos de un protocolo de capa 3 del modelo OSI, desde una red lógica hacia otra red lógica, basado en las tablas de ruta y protocolos de ruta.
- FEC: Forward Error Correction. Corrección de errores hacia adelante.

- FTP: File Transfer Protocol. Protocolo de Transferencia de Archivos. Es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten la transferencia FTP. Permite las transferencias bidireccionales de archivos binarios y archivos ASCII.
- Giga Ethernet: Tecnología de capa 2 del modelo OSI. Basado en la tecnología Ethernet y cuya velocidad de envío de datos es de 1000Mbps
- GPON: Gigabit over passive optical network. Red óptica de la última milla, parte de la familia de redes FTTH-PON que posibilita la explotación de las redes PON.
- GVRP:Generic VLAN Registration Protocol. Protocolo que descubre automáticamente las VLAN existentes en un sistema para ser dados de alta en conmutador de datos principal.
- HDSL: Línea del Suscriptor Digital de Alta Velocidad, tecnología tipo VDSL.
- HTTP: Hypertext Transfer Protocol. Protocolo de transferencia de hipertexto. Funciona con la World Wide Web.
- HTTPS: HTTP Seguro. Protocolo de transferencia de hipertexto seguro. Funciona con la World Wide Web.
- IAB: Consejo de la arquitectura de Internet. Organización de presencia internacional que se encarga administrar y gestionar la Internet así como su crecimiento.
- IDS: Sistema detector de intrusos. Sistema que detecta ataques a una red de datos.
- IDSL: Línea del suscriptor digital ISDN. Es una tecnología del tipo DSL para la última milla de un abonado o usuario.
- IEEE: Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y de Electrónica): Una sociedad internacional de ingeniería con más de 300,000 miembros en 130 países. Sus miembros son profesionales técnicos y científicos con intereses específicos en las áreas de ingeniería electrónica y eléctrica.
- IEEE 802.11: IEEE Committeefor Wireless LANs (Comité para normas de LANs Inalámbricos). Este comité inició el desarrollo de las especificaciones
- PHY y MAC para redes de área local inalámbricas.

- IEEE 802.3 (Ethernet): El más popular de varios tipos de LAN, usualmente usados en computadoras y servidores para tener acceso a redes. Método de acceso para el protocolo de red de área local (LAN) extensamente usado y normalizado por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).
- IEEE 802.3af: Norma para la alimentación remota de dispositivos Ethernet a través de infraestructura LAN. El estándar define las especificaciones de la transferencia de energía eléctrica a través de cables Ethernet estándares y estipula el modo de diseño de equipos de alimentación eléctrica Ethernet y de terminales alimentadas.
- IEEE 802.3az: Norma de ahorro de energía eléctrica.
- IEEE 802.3u (Fast Ethernet): Norma de mejoras de Ethernet, como su velocidad, modo duplex y control de flujo. Especificación del conmutador de datos.
- IEEE 802.1p: Norma para autentificación de usuarios. Implementada a nivel dispositivo de capa 2 del modelo OSI.
- IEEE 802.1q (VLAN): Norma para crear LAN Virtuales en conmutadores de datos del tipo Ethernet para separar tráfico de datos.
- IEEE 802.3i: 10 Mbit/s sobre par trenzado no blindado (UTP). Longitud máxima del segmento 150 metros.
- IEEE 802.1s: Norma del el Algoritmo de Árbol de Expansión (STA) por VLAN.
- IEEE 802.1t: Norma que especifica valores que se usan en el Algoritmo de Árbol de Expansión (STA).
- IEEE 802.1w: Norma del el Algoritmo de Árbol de Expansión Rápido (RSTA), es una mejora del Algoritmo de Árbol de Expansión para que la convergencia de la red más rápido.
- IEEE 802.3x: Norma que establece mecanismos de control de flujo en tecnologías Ethernet.
- IETF: Fuerza de Trabajo de Ingenieros de Internet. Este comité pertenece a la IAB.
- IGMP: Protocolo de Administración de Grupos de Internet. Protocolo que detecta grupos de multidifusión para que los paquetes destinados a estos grupos solo se reenvíen a puertos en donde existan miembros de dichos grupos.
- IPS: Sistema Preventor de Intrusos. Dispositivo que detecta y bloquea ataques a una red de datos.

- IP: Internet Protocol. Protocolo de Internet. Un estándar de la Organización Internacional de Estándares (ISO) que implementa la capa 3 de red de un modelo de sistema abierto de interconexión (OSI) que contiene la dirección de red y es utilizada cuando dirigen un mensaje a una red diferente.
- IP ToS: Método de marcado de paquetes IP para dar prioridad a uno paquetes sobre otros. Este método solo permite hasta 8 clasificaciones por paquete. El marcado se hace en el campo ToS del encabezado IP.
- IP 65/66/67: Establece un nivel de protección contra partículas y agua que puede tener un dispositivo.
- Latencia: retardo que se produce entre el tiempo en que una trama comienza a dejar el dispositivo origen y el tiempo en que la primera parte de la trama llega a su destino.
- LAN: Local Area Network. Red de área local.
- LOS: Line of sight. Línea de vista.
- Modelo OSI: Modelo de referencia de Interconexión de Sistemas Abiertos. es un marco que se puede utilizar para comprender cómo viaja la información a través de una red. El modelo de referencia OSI explica de qué manera los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red.
- Modelo TCP/IP: El modelo TCP/IP es parecido al modelo OSI con la diferencia que las capas 5, 6 y 7 se funden en una sola llamada capa de aplicación.
- Multiplexación: Proceso reversible destinado a reunir señales de varias fuentes distintas, dando una señal compuesta única, para la transmisión por un canal de transmisión común; este proceso equivale a dividir el canal común en distintos canales para transmitir señales independientes en el mismo sentido.
- MTU: Unidad de máxima transferencia. Define el tamaño máximo de trama o segmento que un dispositivo de conectividad puede reenviar.
- NIU: Unidad de Interfaz de red. Normalmente es la tarjeta de red de una computadora personal.
- NLOS: Non- Line of sight. Sin línea de vista.
- NT: Terminación de red.

- OFDM: Multiplexación por División de Frecuencia Ortogonal. Modulación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información.
- OLOS: Obstructed Line of Sight. Línea de vista obstruida.
- OLT:Terminación de línea óptica.
- ONU: Unidad óptica de red.
- ONT: Terminación de red óptica.
- OSPF: (Protocolo primero de la ruta libre más corta). Es un protocolo de enrutamiento interior de estado del enlace.
- PIM-SM: Es un protocolo de enrutamiento para paquetes del tipo multidifusión entre los destinos tipo multidifusión.
- PIRE: Potencia Isotrópica Radiada Efectiva.
- PMI: Punto de monitoreo Inteligente.
- PPPoE: Protocolo punto a punto sobre Ethernet.
- PoE: Integra energía eléctrica una infraestructura de cableado y elimina la necesidad de disponer de corriente alterna en todos lados. La energía y los datos se integran en el mismo cable, soportando desde la categoría 5/5e hasta 100 metros.
- PON: Passive Optical Network. Red óptica pasiva. Permite eliminar todos los componentes activos existentes entre la ONU y la OLT introduciendo en su lugar componentes ópticos pasivos para guiar el tráfico por la red, cuyo elemento principal es el dispositivo divisor óptico “splitter”.
- PTM: Punto multipunto.
- PTP: Punto a punto.
- QPSK: Quadrature Phase-Shift Keying. Desplazamiento de fase en cuadratura.
- RADIUS: RemoteAuthentication Dial-In User Service. Servicio de usuario de marcación de autentificación a distancia.
- Red Troncal (backbone): Término aplicado a una red de datos que une a varias subredes de datos.
- RIP: Protocolo de información de enrutamiento. Protocolo de enrutamiento vector-distancia que utiliza el número de saltos como métrica para determinar la dirección y la distancia a cualquier subred IP.

- RMON: Sondas de monitoreo remoto. Protocolo que define funciones de monitoreo y un conjunto de MIB
- RSSI: Indicador de fuerza de señal recibida. Received Signal Strength Indication. Es una escala de referencia para medir el nivel de potencia de las señales recibidas por un dispositivo en las redes inalámbricas.
- SDSL: Servicio de la línea del suscriptor Digital (DSL) que proporciona igual ancho de banda para subida y bajada de datos.
- SFP: Transceptor de factor de forma pequeño conectable. Son módulos que proporcionan diferentes tipos medios de conexión como son el UTP y la fibra óptica y que son insertados en conmutadores de datos.
- SNMP: Protocolo simple de administración de red. es un protocolo que provee una manera de monitorear y controlar los dispositivos de red y de administrar las configuraciones, la recolección de estadísticas, el desempeño y la seguridad. El SNMP permite que los administradores de red administren el rendimiento de la red, detecten y solucionen los problemas de red y planifiquen el crecimiento de la red.
- SNTP: Protocolo de tiempo de red simple. Este protocolo permite sincronizar dispositivos de red con base en un servidor de tiempo. Existen clientes y servidores SNTP. Los clientes al momento de iniciar mandarán paquetes de solicitud de tiempo al servidor SNTP y éste contestará.
- SP: Prioridad Estricta. Es un método de administración de colas de prioridad donde los equipos de comunicaciones tiene cierto número de colas o buffer para almacenar tramas y se despacharan unas colas antes que otras dependiendo de su prioridad.
- SSH: Secure shell. Interfaz de línea de comandos para accesos a dispositivos de red al igual que TELNET pero a diferencia de este, el envío de datos está encriptado.
- Syslog: Protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.
- TCP/IP: Transmission Control Protocol/Internet Protocol (Protocolo de Internet/Protocolo de Transmisión de Control). Son las siglas de la familia de

protocolos de Internet. Es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre terminales finales.

- TDM: Time divisionmultiplexing. Multiplexación por división en el tiempo.
- TE: Terminales finales. Por ejemplo las computadoras personales, teléfonos IP, impresoras, etc.
- TELNET: Protocolo de terminal virtual que forma parte del conjunto de protocolos TCP/IP. Permite realizar conexiones a los hosts remotos. Telnet brinda la capacidad de una terminal de red o una conexión remota.
- TFTP: Protocolo trivial de transferencia de archivos. Es un servicio no orientado a conexión que utiliza el Protocolo de datagrama de usuario (UDP).
- Throughput: Velocidad de envío de datos.
- UIT: Unión Internacional de Telecomunicaciones. Organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación – TIC.
- VLAN: LAN virtual. Es un grupo de dispositivos de red que está en un segmento IP, tales como servidores, usuarios y otros recursos, configurado para funcionar como si estuvieran conectados a un mismo segmento de red.
- WRR: Es un método de manejo de colas por prioridades donde a cada cola se le da un tiempo de despacho.
- XDSL: Nombre genérico para las tecnologías DSL como ADSL, IDSL, VDSL, etc.
- 10BASE-T se refiere a la velocidad de transmisión a 10 Mbps. El tipo de transmisión es de banda base o digitalmente interpretada. T significa par trenzado.
- QAM: Modulación de amplitud en cuadratura. Técnica de modulación digital que transporta datos, mediante la modulación de la señal portadora de información tanto en amplitud como en fase.
- 16QAM: Modulación de amplitud en cuadratura de 16 estados.
- 64QAM: Modulación de amplitud en cuadratura de 64 estados.

IV.4.3 Lineamientos Normativos.

IV.4.3.1 Requerimientos Generales para el PMI, Red de Microondas y Redes de Fibra Óptica.

A continuación se describen los requerimientos generales previos a cubrir para la selección del equipo, protocolos de comunicación y demás parámetros que se solicitaran en el sistema de video-vigilancia.

a) Determinación de los anchos de banda a usar en los enlaces.
b) Tipo de medio, topología y equipos a usar.
c) Para los enlaces de microondas (PTP, PMP, suscriptor) se deberá realizar el estudio del enlace de microondas correspondiente; especificando al menos los siguientes parámetros:
    - Potencia de salida utilizada en el cálculo de enlace (no sólo la potencia máxima que pueda utilizar la estación radioeléctrica).
    - Potencia Isotrópica Radiada Efectiva (PIRE, por sus siglas en inglés) (limitada por las disposiciones nacionales e internacionales).
    - Tipo de antena:
        a. PTP, PMP (sectorial/haz amplio).
        b. Incluyendo las características del reflector (tipo, tamaño, etc.).
        c. Tipo de polarización.
        d. Frecuencias de operación de transmisión y recepción en la banda de 4.9 GHz.
        e. Ancho del haz de media potencia, Horizontal.
        f. Ancho del haz de media potencia, Vertical.
        g. Relación frente a espalda (F/B).
        h. Ganancia a baja frecuencia.
        i. Ganancia a media Frecuencia.
        j. Ganancia a alta frecuencia.
        k. Patrón de radiación.

d) En caso de ser medio de fibra óptica, a partir de los requerimientos del sistema y de la información de parte del fabricante del equipo óptico elegido, se requiere realizar el diseño del enlace óptico a través de cálculos o especificaciones del fabricante, para determinar como mínimo:

- Trayectorias así como sus longitudes, número de empalmes, protección del empalme, conectores, acopladores, herrajes así como aditamentos necesarios para asegurar físicamente la fibra óptica.
- Tipo de fibra óptico: MMF o SMF
- Recubrimiento de la fibra óptica de acuerdo al medio donde se instale: instalación subterránea, aérea, en ductos, etc.
- Número de fibras a instalar.
- Longitud de onda a usar en el enlace: 850, 1300, 1550, etc.
- Ancho de banda del enlace, el cual debe satisfacer los requerimientos del sistema.
- Pérdida o atenuación total del enlace debido a la fibra óptica, empalmes y conectores; la cual debe estar de acuerdo con las especificaciones del fabricante del equipo óptico.
- Si se requiere atenuadores.

e) Previo a cualquier instalación se deberá contar con un sistema de energía eléctrica, tierra física, pararrayos y respaldo de energía.

f) Para los enlaces inalámbricos, las frecuencias deberán ser asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.

g) Definir índice de protección para exteriores para los equipos de comunicaciones.

h) Definición de pruebas de los enlaces y equipos de comunicaciones.

i) Los dispositivos instalados en el PMI siempre se conectaran a través de un elemento de red, que comunica al PMI con el centro de control. Los dispositivos instalados en el PMI deberán ser compatibles con el elemento de red.

Lineamientos de diseño.

a) Se deben usar protocolos abiertos de organizaciones de normalización internacionales para garantizar la interoperabilidadde los nuevos sistemas de Video-Vigilancia nuevos.

b) Se debe utilizar protocolos de comunicación para el monitoreo y administración que proporcionen seguridad al envío de la información.

c) Se debe solicitar pruebas de los enlaces.
d) La transmisión de datos deberá realizarse utilizando un algoritmo de cifrado.
e) La estación radioeléctrica deberá estar homologada ante el Instituto Federal de Telecomunicaciones.
f) Se deberán de configurar y gestionar, los elementos de la red, local y remotamente.

IV.4.3.2 Requerimientos Generales para el Centro de Control (Red LAN).

A continuación se presentan los requerimientos previos a la instalación y selección de equipo para la red LAN de un sistema de video-vigilancia.

a) Definir el número de nodos.
b) Definir la ubicación de los nodos.
c) Definir el tipo o tipos de medios: Cable UTP 6 o fibra óptica y tipo de fibra óptica.
d) Tener el plano de trayectorias de cables y de fibra óptica.
e) Definir ubicación y número Sala Principal de Comunicaciones o Sala de Instalaciones de entrada, Salas de Interconexiones Intermedias, Sala de Equipos y/o Sala de Telecomunicaciones.
f) Determinar la cantidad y tipo de equipo a utilizar.
g) Definir las políticas de administración y monitoreo de equipo.
h) Definir las pruebas de los enlaces y equipos de comunicaciones.

IV.4.3.3 Parámetros de Radiocomunicación.

A continuación, se enlistan los parámetros técnicos de la estación radio eléctrica punto a punto, multipunto y la repetidora. Se enlistarán en dicho orden.

a) Estación radio eléctrica punto a punto suscriptor (usualmente el ancho de banda es de 10/25 Mbps).
   - En el enlace de microondas se puede utilizar LOS (Line Of Sight, por sus siglas en inglés) /OLOS (Obstructed Line Of Sight, por sus siglas en inglés) /NLOS (Non Line of Sight, por sus siglas en inglés) en terminal PTP y compatible con

terminal PMP, se podrá escoger cualquier tipo de acuerdo al estudio del enlace.

- Frecuencias asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.
- Modulación dinámica: el equipo de radio frecuencia debe soportar como mínimo los siguientes tipos de modulación BPSK, QPSK, 16QAM, 64QAM.
- Ancho del canal: se podrá usar el ancho de canal que cumpla la regulación aplicable por usuario y a las frecuencias asignadas a la entidad.
- Capacidad del sistema: El ancho de banda *(AB)*mínimo a utilizar se debe calcular con base en la ecuación(1):

$$AB_{Total} = \left(\sum_{n=1}^{m} AB_{cámara\ n} + AB_{voz\ IP} + AB_{altavoz} + AB_{monitoreo\ de\ datos}\right) * c \quad (1)$$

donde:

AB_{Total}: Ancho de banda mínimo utilizado para el enlace al PMI (Punto de Monitoreo Inteligente).

$AB_{cámaran}$: Ancho de banda utilizado por la cámara *n*. Se pueden considerar cámaras fijas y cámaras Pan-Tilt-Zoom (PTZ, por sus siglas en inglés). En el capítulo 3 de este documento se recomienda el ancho de banda mínimo de para una cámara fija o PTZ.

$AB_{voz\ IP}$: Ancho de banda utilizado por la voz IP en el PMI (botón de pánico)

$AB_{altavoz}$: Ancho de banda utilizado por el altavoz en el PMI.

$AB_{monitoreo\ de\ datos}$: Ancho de banda utilizado por los datos de monitoreo de los equipos del PMI.

c: Es una constante de tolerancia y depende del número de cámaras a utilizar. Se recomienda que *c* esté en el intervalo de 1.3 a 1.5.

Todos los elementos de la ecuación (1) están expresados en Mbps.

Recomendación para el uso de la ecuación (1).

El ancho de banda para los componentes $AB_{voz\ IP}$, $AB_{altavoz}$, $AB_{monitoreo\ de\ datos}$ es de 500 kbps (0.5 Mbps).

Ejemplo 1. Sí solo existe una cámara (se supone de 2 Mbps), una terminal de voz IP, un altavoz y datos de monitoreo en el PMI. La constante *c=1.5* y se considera como una tolerancia para asegurar la comunicación y permitiría agregar otra cámara. Por lo tanto el ancho de banda sería (sustituyendo los valores en la ecuación (1)):

$$AB_{Total} = \left(\sum_{n=1}^{1} AB_{cámara\ n} + AB_{voz\ IP} + AB_{altavoz} + AB_{monitoreo\ de\ datos}\right) * 1.5$$

$$AB_{Total} = (2 + 0.5) * 1.5 = 3.75\ Mbps$$

Ejemplo 2. Para un PMI con cuatro cámaras, una terminal de voz IP, un altavoz y los datos de monitoreo, se tiene que para obtener el ancho de banda total se sustituyen los valores en la ecuación (1), con una *c=1.3*:

$$AB_{Total} = \left(\sum_{n=1}^{4} AB_{cámara\ n} + AB_{voz\ IP} + AB_{altavoz} + AB_{monitoreo\ de\ datos}\right) * 1.3$$

$$AB_{Total} = (4(2) + (0.5)) * 1.3 = (8 + 0.5) * 1.3 = 11.05\ Mbps$$

- Debe tener una disponibilidad de al menos 99.991% (que equivale a 47.304 minutos/año).
- Calidad del servicio: La estación radio eléctrica debe soportar las siguientes normas para proveer la calidad de servicio: IEEE 802.1p, IP ToS de acuerdo con RFC791 y DSCP de acuerdo con RFC2474. Con un manejo mínimo de cuatro colas de prioridad.
- Dependiendo del diseño de la red inalámbrica, se debe utilizar una VLAN (red de área local virtual, por sus siglas en inglés) diferente para cada uno de los

servicios (video, voz, administración, etc) y se implementarán de acuerdo a la norma IEEE 802.1q.

- Gestión: De acuerdo a las necesidades de gestión de la estación radio eléctrica, se podrán elegir uno o más de los siguientes protocolos orientados a conexión de gestión de los equipos: HTTPS/SSH/SNMP V2c o V3.

  No se permite los protocolos TELNET y HTTP, en caso de que el equipo los soporte, éstos serán deshabilitados.
- La estación radio eléctrica del PMI se debe configurar y gestionar desde la radio base y remotamente, además de reportar los parámetros operativos más importantes como son RSSI, throughput, estado del enlace, como mínimo. Se debe permitir deshabilitar las funciones de configuración y gestión.
- Potencia de transmisión: Ésta se definirá en el estudio previo de enlace.
- Actualización de software: Las estaciones radio eléctricas deben tener la característica de actualización de firmware de manera local y remota de forma gratuita, a través de los protocolos TFTP/FTP.
- Cifrado de datos: El video y los datos de las terminales finales del PMI serán cifradas usando alguno de los siguientes algoritmos DES, AES 128 bits.
- Interfaz Ethernet IEEE 802.3/IEEE 802.3u. Opcional la capacidad de recibir corriente eléctrica a través del puerto Ethernet (IEEE 802.3af).
- Deberá contar con corrección de errores y mecanismo de retransmisión automática a nivel RF: Forward Error Correction (FEC).
- Latencia Máxima: menor a 6 ms por estación de radio frecuencia. La suma de la latencia debe cumplir con las recomendaciones de latencia para video calculadas de acuerdo a las configuraciones usadas en las cámaras, para evitar efectos de pérdida de resolución o imágenes con retardo.
- Regulación: La estación radioeléctrica deberá estar homologado ante la Instituto Federal de Telecomunicaciones (IFT).
- Alimentación Eléctrica: 110 VCA – 120 VCA a 50 Hz - 60 Hz o vía puerto Ethernet (Power over Ethernet PoE) en cumplimiento con la norma IEEE 802.3af.

- Certificación de índice de protección para exteriores: De acuerdo a las condiciones ambientales de sitio, la estación radioeléctrica debe cumplir con alguno de los siguientes índices de protección: IP 65/66/67.
- Debe de incluir todos los accesorios necesarios para su correcta instalación. Por ejemplo: dispositivo con interface PoE 100BASET/GBE con alimentación externa, cables CAT5e, kit de montaje, etc.
- Posibilidad de crecimiento del sistema sin necesidad de licencias adicionales.
- Alineación de la estación radio eléctrica: Se recomienda contar con una herramienta de alineación entre las antenas, por ejemplo, tono audible.
- Capacidad de enrutamiento: Esto depende de los requerimientos de diseño.
- Protocolos de enrutamiento: Dependiendo de los requerimientos de diseño, en caso de requerir un protocolo de ruteo dinámico abierto se puede usar RIPv2/OSPF o sus versiones superiores.
- Temperatura de operación: los equipos deberán operar en un rango de temperatura de -35 ^{o}C a 60 ^{o}C. Este parámetro puede variar de acuerdo a la región de instalación.
- Se recomienda la posibilidad de contar con sincronización de la antena vía GPS/SNTP.
- Humedad de operación: La aplicación de este parámetro depende de la zona geográfica en la que se instale el sistema.

b) Estación radio eléctrica PMP: la capacidad del enlace en Mbps dependerá del ancho de banda calculado a partir del número de suscriptores (usualmente de 50 Mbps).
   - En el enlace de microondas se puede utilizar LOS/OLOS/NLOS (Línea de Vista /Línea de Vista Obstruida/ Sin Línea de Vista) en terminal PTP (Punto a Punto) y compatible con terminal PMP (Punto Multi Punto). Se podrá escoger cualquier tipo de acuerdo al estudio de enlace.
   - Frecuencias asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.
   - Tipo de antena: sectorial/haz amplio.

- Método de multiplexaje: TDM/OFDM (dependiendo de las necesidades del usuario se podrá utilizar MIMO). El método de multiplexaje debe ser el mismo en todos los elementos del enlace de microondas (PTP y suscriptores).
- Esquema de duplexaje: TDD/FDD. El esquema de duplexaje debe ser el mismo en todos los elementos del enlace de microondas (PTP y suscriptores).
- Modulación adaptativa: el equipo de radio frecuencia debe soportar como mínimo los siguientes tipos de modulación BPSK, QPSK, 16QAM, 64QAM.
- Ancho del canal: se podrá usar cualquier ancho de canal cumpliendo la regulación aplicable por usuario y a las frecuencias asignadas a la entidad.
- Capacidad del sistema: El ancho de banda mínimo a utilizar se calcula con base en la ecuación (2):

$$AB_{PMP} = \left(\sum_{n=1}^{k} AB_{Total} \right) * c_1 \qquad (2)$$

donde:

AB_{PMP}: Ancho de banda mínimo utilizado para el enlace PMP.

AB_{Total}: Ancho de banda utilizado por el enlace de cada suscriptor *k*.

c_1: Es una constante de tolerancia para asegurar la comunicación y depende del número de suscriptores. Se recomienda que c_1 se considere igual a 1.3.

Todos los elementos de la ecuación (2) están expresados en Mbps.

Recomendación para el uso de la ecuación (2).

Ejemplo 3. Tomando como referencia la figura IV.4.1 y los datos del ejemplo 2 de la ecuación (1), el ancho de banda para un PMI es de 11.05 Mbps. Si se tienen cuatro PMI, para obtener el ancho de banda total del enlace PMP, se sustituyen los valores en la ecuación (2):

$$AB_{PMP} = \left(\sum_{n=1}^{4} AB_{Total}\right) * 1.3$$

$$AB_{PMP} = (4 * 11.05) * 1.3 = 57.46\ Mbps$$

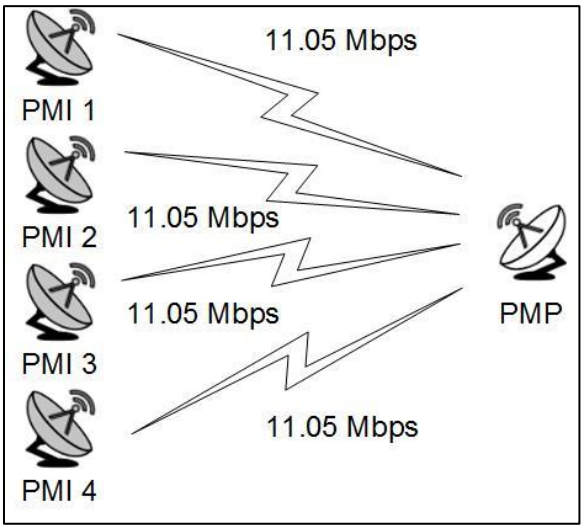


Figura IV.4.1. Diagrama a bloques del cálculo del ancho de banda de un enlace punto a punto

- Enlace inalámbrico PTP en este caso deberá ser de alta capacidad y debe tener una disponibilidad de al menos del 99.991% (que equivale a 47.304 minutos/año).
- Calidad del servicio: La estación radio eléctrica debe soportar las siguientes normas para proveer la calidad de servicio: IEEE 802.1p, IP ToS de acuerdo con RFC791 y DSCP de acuerdo con RFC2474.Con un manejo mínimo de cuatro colas de prioridad.
- Dependiendo del diseño de la red inalámbrica, en caso de requerir el uso de VLAN (red de área local virtual, por sus siglas en inglés), se implementarán de acuerdo a la norma IEEE 802.1q.
- Gestión: De acuerdo a las necesidades de gestión de la estación radio eléctrica se podrán elegir uno o más de los siguientes protocolos orientados a conexión de gestión de los equipos: HTTPS/SSH/SNMP V2c o V3. No se permite los

protocolos TELNET y HTTP, en caso de que el equipo los soporte, éstos serán deshabilitados.

- La estación radio eléctrica del enlace PTP de alta capacidad se debe configurar y gestionar desde la radio base y remotamente, además de reportar los parámetros operativos más importantes como son RSSI, throughput, estado del enlace como mínimo. Se debe permitir deshabilitar las funciones de configurar y gestionar.
- Potencia de transmisión: Ésta se definirá en el estudio previo de cálculo de enlace.
- Actualización de software: Las estaciones radio eléctricas deben de tener la característica de actualización de firmware de manera local y remota de forma gratuita, a través de los protocolos TFTP/FTP.
- Cifrado de datos: El video y los datos de las terminales finales del PMI serán cifradas usando alguno de los siguientes algoritmos DES, AES 128 bits.
- Interfaz Ethernet IEEE 802.3/IEEE 802.3u. Opcional la capacidad de recibir corriente eléctrica a través del puerto Ethernet (IEEE 802.3af).
- Deberá contar con corrección de errores y mecanismo de retransmisión automática a nivel RF: Forward Error Correction (FEC).
- Latencia Máxima: menor a 6 ms por estación de radio frecuencia. La suma de la latencia debe cumplir con las recomendaciones de latencia para video calculadas de acuerdo a las configuraciones usadas en las cámaras para evitar efectos de pérdida de resolución o imágenes con retardo.
- Regulación: La estación radioeléctrica deberá estar homologado ante la Instituto Federal de Telecomunicaciones (IFT).
- Alimentación Eléctrica: 110 VCA – 120 VCA, 50 Hz - 60 Hz o vía puerto Ethernet en cumplimiento con la norma IEEE 802.3af
- Certificación de índice de protección para exteriores: De acuerdo a las condiciones ambientales de sitio, la estación radioeléctrica debe cumplir con alguno de los siguientes índices de protección: IP 65/66/67.
- Debe de incluir todos los accesorios necesarios para su correcta instalación. Por ejemplo: dispositivo con interface POE 100BASET/GBE con alimentación externa, cables CAT5e, kit de montaje, etc.

- Posibilidad de crecimiento del sistema sin necesidad de licencias adicionales.
- Alineación de la estación radio eléctrica: Se recomienda contar con una herramienta de alineación entre las antenas, por ejemplo, tono audible.
- Capacidad de enrutamiento: Esto depende de los requerimientos de diseño.
- Protocolos de enrutamiento: Dependiendo de los requerimientos de diseño, en caso de requerir un protocolo de ruteo dinámico abierto se puede usar RIPv2/OSPF o sus versiones superiores.
- Temperatura de operación: los equipos deberán operar en un rango de temperatura de -35 ^{o}C a 60 ^{o}C. Este parámetro puede variar de acuerdo a la región de instalación.
- Se recomienda la posibilidad de tener sincronización de la antena vía GPS/SNTP.
- Humedad de operación: La aplicación de este parámetro depende de la zona geográfica en la que se instale el sistema.

c) Estación radio eléctrica PTP de alta capacidad, la capacidad del enlace en Mbps dependerá del ancho de banda calculado a partir de los puntos de agregación (usualmente de 250 Mbps).

- Líneas de vista LOS/OLOS/NLOS en terminal PTP (Punto a Punto) y compatible con terminal PMP (Punto MultiPunto).Se podrá escoger cualquier tipo de acuerdo al estudio de enlace.
- Frecuencias asignadas por el Instituto Federal de Telecomunicaciones (IFT) para uso exclusivo de seguridad pública en los tres órdenes de gobierno. No se permite el uso de frecuencias libres o de otro tipo de asignaciones.
- Método de multiplexaje: TDM/OFDM
- Modulación adaptativa: el equipo de radio frecuencia debe soportar como mínimo los siguientes tipos de modulación BPSK, QPSK, 16QAM, 64QAM.
- Ancho del canal: se podrá usar cualquier ancho de canal cumpliendo la regulación aplicable por usuario y a las frecuencias asignadas a la entidad.
- Capacidad del sistema: El ancho de banda mínimo a utilizar se calcula con base en la ecuación (3):

$$AB_{PTP\ alta\ capacidad} = \left(\sum_{n=1}^{l} AB_{Total\ l}\right) * c_2 \qquad (3)$$

donde:

$AB_{PTP\ alta\ capacidad}$: Ancho de banda mínimo utilizado para el enlace PTP de alta capacidad.

AB_{Total}: Ancho de banda utilizado por el enlace de cada PMP.

c_2: Es una constante de tolerancia que se considera para asegurar la comunicación y depende del número de suscriptores. Se recomienda que c_2 se considere igual a 1.3.

Todos los elementos de la ecuación (3) están expresados en Mbps.

Recomendación para el uso de la ecuación (3).

Ejemplo 4. Tomando como referencia la figura IV.4.2, se tienen diez PMI y 3 PTP. Del PMI 1 al PMI 4 están conectados al PMP 1, el PMI 5 y el PMI 6 están conectados el PMP 2, y del PMI 7 al PMI 10 se encuentran conectados al PMP 3. El ancho de banda total del enlace PTP de alta capacidad se determina sustituyendo los valores en la ecuación (3):

$$AB_{PTP\ alta\ capacidad} = \left(\sum_{n=1}^{3} AB_{Total\ l}\right) * c_2$$

$$AB_{PTP} = (57.46 + 28.73 + 57.46) * 1.3 = 143.65\ Mbps$$

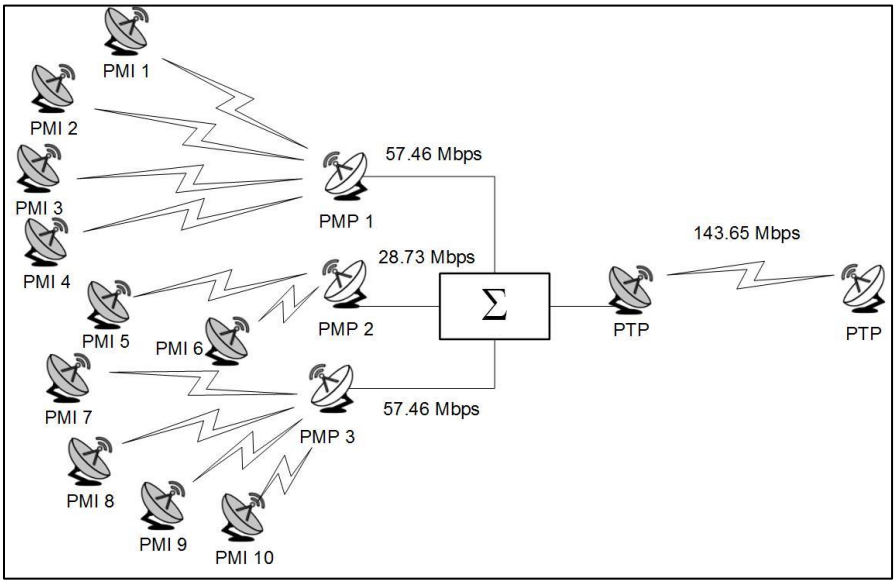


Figura IV.4.2 Diagrama a bloques del cálculo del ancho de banda de un enlace punto a punto de alta capacidad

- Enlace inalámbrico punto-punto en este caso deberá ser de alta capacidad y debe tener una disponibilidad de al menos del 99.991% (que equivale a 47.304 minutos/año).
- Calidad del servicio: La estación radio eléctrica debe soportar las siguientes normas para proveer la calidad de servicio: IEEE 802.1p, IP ToS de acuerdo con RFC791 y DSCP de acuerdo con RFC2474. Con un manejo mínimo de cuatro colas de prioridad.
- Dependiendo del diseño de la red inalámbrica, en caso de requerir el uso de VLAN (red de área local virtual, por sus siglas en inglés), se implementarán de acuerdo a la norma IEEE 802.1q.
- Gestión: De acuerdo a las necesidades de gestión de la estación radio eléctrica se podrán elegir uno o más de los siguientes protocolos orientados a conexión de gestión de los equipos: HTTPS/SSH/SNMP V2c o V3. No se permite los protocolos TELNET y HTTP, en caso de que el equipo los soporte, éstos serán deshabilitados.
- La estación radio eléctrica del enlace punto a punto de alta capacidad se debe de configurar y gestionar desde la radio base y remotamente, además de reportar los parámetros operativos más importantes como son RSSI,

throughput, estado del enlace como mínimo. Se debe permitir deshabilitar las funciones de configurar y gestionar.

- Potencia de transmisión: Ésta se definirá en el estudio de enlace.
- Actualización de software: Las estaciones radio eléctricas deben de tener la característica de actualización de firmware de manera local y remota de forma gratuita, a través de los protocolos TFTP/FTP.
- Cifrado de datos: El video y los datos de las terminales finales del PMI serán cifradas usando alguno de los siguientes algoritmos DES, AES 128 bits.
- Interfaz Ethernet IEEE 802.3/IEEE 802.3u. Opcional la capacidad de recibir corriente eléctrica a través del puerto Ethernet (IEEE 802.3af).
- Deberá contar con corrección de errores y mecanismo de retransmisión automática a nivel RF: Forward Error Correction (FEC).
- Latencia Máxima: menor a 6 ms por estación de radio frecuencia. La suma de la latencia debe cumplir con las recomendaciones de latencia para video calculadas de acuerdo a las configuraciones usadas en las cámaras para evitar efectos de pérdida de resolución o imágenes con retardo.
- Regulación: La estación radioeléctrica deberá estar homologado ante la Instituto Federal de Telecomunicaciones (IFT).
- Alimentación Eléctrica: 110 VCA – 120 VCA, 50 Hz - 60 Hz o vía puerto Ethernet en cumplimiento con la norma IEEE 802.3af.
- Certificación de índice de protección para exteriores: De acuerdo a las condiciones ambientales de sitio, la estación radioeléctrica debe cumplir con alguno de los siguientes índices de protección: IP 65/66/67.
- Debe de incluir todos los accesorios necesarios para su correcta instalación. Por ejemplo: dispositivo con interface POE 100BASET/GBE con alimentación externa, cables CAT5e, kit de montaje, etc.
- Posibilidad de crecimiento del sistema sin necesidad de licencias adicionales.
- Alineación de la estación radio eléctrica: Se recomienda contar con una herramienta de alineación entre las antenas, por ejemplo, tono audible.
- Capacidad de enrutamiento: Esto depende de los requerimientos de diseño.

- Protocolos de enrutamiento: Dependiendo de los requerimientos de diseño, en caso de requerir un protocolo de ruteo dinámico abierto se puede usar RIPv2/OSPF o sus versiones superiores.
- Temperatura de operación: los equipos deberán operar en un rango de temperatura de -35°C a 60°C. Este parámetro puede variar de acuerdo a la región de instalación.
- Se recomienda la posibilidad de tener sincronización de la antena vía GPS/SNTP.
- Humedad de operación: La aplicación de este parámetro depende de la zona geográfica en la que se instale el sistema.

d) Enrutador y Conmutador de datos en el PMI

El conmutador de datos en el PMI podrá ser un equipo no administrable o administrable, dependiendo de los requerimientos del diseño. El conmutador de datos y el enrutador deberán cumplir, en caso de que sean administrables, con protocolos y normas establecidos por la IEEE y la IETF.

Para el enrutador y de acuerdo a los requerimientos del diseño, se escogerán los protocolos que apliquen.

- Puertos o interfaces de tecnología: IEEE 802.3/802.3u.
- Soporte a protocolos IPv4 e IPv6: Debe cumplir con los RFC 791, 1349 y 6864 para IPv4; y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722.
- Direcciones primarias y/o secundarias por interfaz o VLAN (802.1q): Los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. Es opcional que además de poder asignar una primera dirección IP, se pueda asignar direcciones IP secundarias extra, esto depende del diseño o requerimientos.
- Rutas estáticas: Los equipos con capacidades de enrutamiento deben tener la posibilidad de configurar manualmente rutas para llenar su tabla de enrutamiento.
- Protocolo de ruteo dinámico RIPv2 y OSPF para IPv4 e IPv6. El protocolo de ruteo dinámico RIP debe cumplir con lo especificado en el RFC 2453 y el RFC 2080 y es recomendable para redes pequeñas cuando subredes están a no más

de 15 enrutadores de separación. Para el caso de OSPF debe cumplir con el RFC 2328 y el RFC 5340 y se recomienda cuando el número de subredes supera a las limitantes de RIP v2.

- DHCP: Debe cumplir con el RFC 2131 y el RFC 3046. Un equipo con capacidades de enrutamiento puede ser un servidor DHCP, cliente DHCP y/o DHCP de reenvío. El servidor DHCP nos permite asignar direcciones IP de host a los clientes DHCP. El cliente DHCP en un enrutador permite que a sus interfaces se le asigne una dirección IP por medio de un servidor DHCP. El DHCP de reenvío manda las peticiones de clientes DHCP al servidor DHCP.
- IGMP: Debe cumplir con el RFC 2236. Este protocolo permite que todos los grupos multicast sean anunciados a los protocolos de ruteo multicast.
- PIM-SM: Debe cumplir con el RFC 7761. Permite el ruteo multicast.
- DVMRP. Debe cumplir con los RFC 1075 y 2715. Permite el enrutamiento con direcciones IP multicast.
- SNTP: Deberá cumplir con el RFC 4330. Usado cuando se requiere que los equipos sincronicen su reloj tomándolo de un servidor de tiempo.
- QoS DSCP/Precedencia IP: Protocolo que utiliza el marcado de paquetes IP en el campo TOS del encabezado que permite darle un tratamiento para priorizar tramas.
- IEEE 802.1q: Norma que describe el funcionamiento, formatos de paquetes y parámetros de las VLAN.
- IEEE 802.3x: Norma que establece un mecanismo de control de flujo para así evitar congestionamientos.
- SNMPv2c/v3: Protocolo que permite el monitoreo de dispositivos de red.
- SSHv2: Protocolo que permite el acceso remoto a un equipo de red de forma segura vía línea de comandos.
- FTP/TFTP Cliente: Protocolos que permiten la transferencia de archivos. Usual para actualizar firmware o archivos de configuraciones o respaldarlos.
- Syslog: Protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.
- RMON: Protocolo que da un conjunto de variables o MIB´s para el monitoreo de red así como un protocolo para la consulta de estos MIB´s.

- HTTPS: Protocolo basado en hipertexto para el monitoreo de un dispositivo de red de forma segura. A diferencia de HTTP la transmisión de datos viaja de forma cifrada gracias a la implementación de los protocolos SSL y TLS.

  No se permite el uso de Telnet y HTTP, en caso de que el equipo tenga implementado estos protocolos, deberán ser deshabilitados. Las aplicaciones aquí recomendadas son para fines de administración y actualización de equipo.
- El enrutador debe de cumplir con las especificaciones del medio ambiente, tales como temperatura y humedad, cuyos valores dependerán de la zona donde serán instalados. Cumplirá con el estándar EN 55022/EN 55024 o similares, para garantizar inmunidad ante descargas electrostáticas e interferencias de radiofrecuencia. Además será un equipo diseñado para uso industrial o en exteriores, por lo que debe de cumplir con la norma IP51 como mínimo o similares, considerando que el gabinete que lo contenga le dará protección del medio ambiente.
- El equipo deberá soportar actualizaciones de firmware vía remota y local.

Para el conmutador de datos y de acuerdo a los requerimientos del diseño, se escogerán los protocolos que apliquen.

- Puertos o interfaces de tecnología: IEEE 802.3/802.3u.
- Soporte a protocolos IPv4 e IPv6: Debe cumplir con los RFC 791, 1349 y 6864 para IPv4; y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722.
- Direcciones primarias y/o secundarias por interfaz o VLAN (802.1q): Los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. Es opcional que además de poder asignar una primera dirección IP, se pueda asignar direcciones IP secundarias extra, esto depende del diseño o requerimientos.
- IGMP: Debe cumplir con el RFC 2236. Este protocolo permite que todos los grupos multicast sean anunciados e identifican sus miembros en los puertos de un conmutador de datos.
- SNTP: Deberá cumplir con el RFC 4330. Usado cuando se requiere que los equipos sincronicen su reloj tomándolo de un servidor de tiempo.

- QoS DSCP/Precedencia IP: Protocolo que utiliza el marcado de paquetes IP en el campo TOS del encabezado que permite darle un tratamiento para priorizar tramas.
- IEEE 802.1q: Norma que describe el funcionamiento, formatos de paquetes y parámetros de las VLAN.
- IEEE 802.1p: Norma que define un método para marcar y dar tratamiento a tramas para fines de calidad de servicio.
- IEEE 802.3x: Norma que establece un mecanismo de control de flujo para así evitar congestionamientos.
- IEEE 802.3af: Norma que regula la alimentación que puede recibir o dar un equipo a través de los puertos de Ethernet.
- IEEE 802.3az: Norma que regula el ahorro de energía.
- IEEE 802.1Qau: Norma que establece mecanismos para evitar la congestión en redes de alto uso de ancho de banda.
- SNMPv2c/v3: Protocolo que permite el monitoreo de dispositivos de red.
- SSHv2: Protocolo que permite el acceso remoto a un equipo de red de forma segura vía línea de comandos.
- FTP/TFTP Cliente: Protocolos que permiten la transferencia de archivos. Usual para actualizar firmware o archivos de configuraciones o respaldarlos.
- Syslog: Protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.
- RMON: Protocolo que da un conjunto de variables o MIB´s para el monitoreo de red así como un protocolo para la consulta de estos MIB´s.
- HTTPS: Protocolo basado en hipertexto para el monitoreo de un dispositivo de red de forma segura. A diferencia de HTTP la transmisión de datos viaja de forma cifrada gracias a la implementación de los protocolos SSL y TLS.

  No se permite el uso de Telnet y HTTP, en caso de que el equipo tenga implementado estos protocolos, deberán ser deshabilitados. Las aplicaciones aquí recomendadas son para fines de administración y actualización de equipo.
- El conmutador de datos debe de cumplir con las especificaciones del medio ambiente, tales como temperatura y humedad, cuyos valores dependerán de la zona donde serán instalados. Cumplirá con el estándar EN 55022/EN 55024 o

similares, para garantizar inmunidad ante descargas electrostáticas e interferencias de radiofrecuencia. Además será un equipo diseñado para uso industrial o en exteriores, por lo que debe de cumplir con la norma IP51 como mínimo o similares, considerando que el gabinete que lo contenga le dará protección del medio ambiente.

- El equipo deberá soportar actualizaciones de firmware vía remota y local.

IV.4.3.4 Parámetros de los Dispositivos de la Red de Fibra Óptica.

a) PMI: El conmutador de datos en el PMI podrá ser un equipo no administrable o administrable, dependiendo de los requerimientos del diseño. El conmutador de datos y el enrutador deberán cumplir, en caso de que sean administrables, con protocolos y normas establecidos por la IEEE y la IETF. A continuación se enlistan los protocolos más usuales. De acuerdo a los requerimientos del diseño, se escogerán los que apliquen.
   - Puertos o interfaces de tecnología: IEEE 802.3/802.3u.
   - Puertos SFP para realización de enlaces con otros dispositivos de comunicaciones que no estén en el PMI. La tabla IV.4.1 es una referencia de la distancia de cada tipo de SFP.

Tabla IV.4.1 Referencia de la distancia de cada tipo de SFP

SFP	Tipo de Fibra óptica / Longitud de Onda	Medida de la fibra (µm)	Ancho de banda por km (MHz-km)	Distancia máxima de operación
100BaseFX	MMF/1310nm	50	500	5 km
		62.5		2 km
100BaseSX	MMF/850	50	500	550 m
		62.5	200	300 m
100BaseLX	SMF			10 km
100BaseEX	SMF			40 km
100BaseZX	SMF			80 km
1000BaseSX	MMF/850	62.5	160	220 m
			200	275 m
		50	400	500 m
			500	550 m

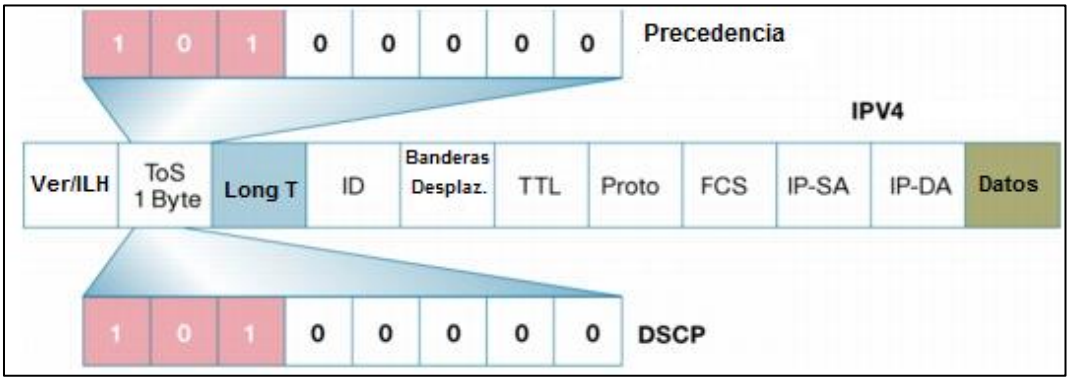
			2000	1 km
1000BaseLX/LH	SMF/1310			10 km a 20 km
1000BaseEX	SMF/1310			20 km a 40 km
1000BaseZX	SMF/1550			80 km
10GBaseSR	MMF/850	62.5	160	26 m
			200	33 m
		50	400	66 m
			500	82 m
			2000	300 m
10GBaseLR	SMF/1310			10 km
10GBaseER	SMF/1550			40 km

- Soporte a protocolos IPv4 e IPv6: Debe cumplir con los RFC 791, 1349 y 6864 para IPv4; y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722.
- Direcciones primarias y/o secundarias por interfaz o VLAN (802.1q): Los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. Es opcional que además de poder asignar una primera dirección IP, se pueda asignar direcciones IP secundarias extra, esto depende del diseño o requerimientos.
- Rutas estáticas: Los equipos con capacidades de enrutamiento deben tener la posibilidad de configurar manualmente rutas para llenar su tabla de enrutamiento.
- Protocolo de ruteo dinámico RIPv2 y OSPF para IPv4 e IPv6. El protocolo de ruteo dinámico RIP debe cumplir con lo especificado en el RFC 2453 y el RFC 2080y es recomendable para redes pequeñas cuando subredes están a no más de 15 enrutadores de separación. Para el caso de OSPF debe cumplir con el RFC 2328 y el RFC 5340 y se recomienda cuando el número de subredes supera a las limitantes de RIP v2.
- DHCP: Debe cumplir con el RFC 2131 y el RFC 3046. Un equipo con capacidades de enrutamiento puede ser un servidor DHCP, cliente DHCP y/o DHCP de reenvío. El servidor DHCP nos permite asignar direcciones IP de host a los clientes DHCP. El cliente DHCP en un enrutador permite que a sus interfaces se le asigne una dirección IP por medio de un servidor DHCP. El DHCP de reenvío manda las peticiones de clientes DHCP al servidor DHCP.
- IGMP: Debe cumplir con el RFC 2236. Este protocolo permite que todos los grupos multicast sean anunciados a los protocolos de ruteo multicast, en el caso

de los enrutadores, o sean identificados sus miembros en los puertos de un conmutador de datos.

- PIM-SM: Debe cumplir con el RFC 7761. Permite el ruteo multicast.
- DVMRP. Debe cumplir con los RFC 1075 y 2715. Permite el enrutamiento con direcciones IP multicast.
- SNTP: Deberá cumplir con el RFC 4330. Usado cuando se requiere que los equipos sincronicen su reloj tomándolo de un servidor de tiempo.
- QoS DSCP/Precedencia IP: Protocolo que utiliza el marcado de paquetes IP en el campo ToS del encabezado que permite darle un tratamiento para priorizar tramas. En la figura IV.4.3 se muestra el encabezado IP, donde se hace el marcado para priorizar paquetes IP. Como muestra la figura se hace en el campo ToS (Tipo de Servicio), el cual se puede manejar de dos formas. La primera es tomando los tres primeros bits para grabar un valor entre 0 y 7, llamado Precedencia, y mientras más alto más prioridad tiene el paquete IP. La segunda forma es manejar los ocho bits del campo ToS para grabar un valor DSCP (Punto de código de servicios diferenciados), su valor es una combinación entre Precedencia más un tipo de servicio.

Figura. IV.4.3 QoS en encabezado IP



- IEEE 802.1q: Norma que describe el funcionamiento, formatos de paquetes y parámetros de las VLAN.
- IEEE 802.1p: Norma que define un método para marcar y dar tratamiento a tramas para fines de calidad de servicio.
- IEEE 802.3x: Norma que establece un mecanismo de control de flujo para así evitar congestionamientos.
- IEEE 802.3af: Norma que regula la alimentación que puede recibir o dar un equipo a través de los puertos de Ethernet.
- IEEE 802.3az: Norma que regula el ahorro de energía.
- IEEE 802.1Qau: Norma que establece mecanismos para evitar la congestión en redes de alto uso de ancho de banda.
- SNMPv2c/v3: Protocolo que permite el monitoreo de dispositivos de red.
- SSHv2: Protocolo que permite el acceso remoto a un equipo de red de forma segura vía línea de comandos.
- FTP/TFTP Cliente: Protocolos que permiten la transferencia de archivos. Usual para actualizar firmware o archivos de configuraciones o respaldarlos.
- Syslog: Protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.
- RMON: Protocolo que da un conjunto de variables o MIB´s para el monitoreo de red así como un protocolo para la consulta de estos MIB´s.
- HTTPS: Protocolo basado en hipertexto para el monitoreo de un dispositivo de red.

No se permite el uso de Telnet y HTTP, en caso de que el equipo tenga implementado estos protocolos, deberán ser deshabilitados. Las aplicaciones aquí recomendadas son para fines de administración y actualización de equipo.

- El enrutador o conmutador de datos debe de cumplir con las especificaciones del medio ambiente, tales como temperatura y humedad, cuyos valores dependerán de la zona donde serán instalados. Cumplirá con el estándar EN 55022/EN 55024 o similares, para garantizar inmunidad ante descargas electrostáticas e interferencias de radiofrecuencia. Además, será un equipo diseñado para uso industrial, por lo que debe de cumplir con la norma IP30 como mínimo o similares, considerando que el gabinete que lo contenga le dará protección del medio ambiente.
- La alimentación de energía eléctrica debe de ser de 110 V a 120 V, a la frecuencia de 50 Hz a 60 Hz.

Se debe solicitar que la memoria técnica incluya pruebas de transferencia de diversos MTU, pruebas de retardo y pruebas de pérdida de paquete, en conformidad con el RFC 2544.

En caso de que existiese equipo XDSL en el PMI, dependiendo del diseño del sistema, podrá incluir las siguientes características, además de las anteriores:

- PPPoE
- Ruteo estático
- Se debe de configurar y gestionar local y remotamente, además de reportar los parámetros operativos más importantes, como por ejemplo, el estado del enlace de la red de acceso.
- Monitoreo y administración vía TR069. Protocolo de administración aceptado por DSL Forum. TR069 define un conjunto de estructuras del sistema de gestión de red, incluyendo “modelo de gestión”, “interfaz interactiva” y “parámetros de gestión”. TR069 completa principalmente las siguientes funciones: configuración automática y de servicios dinámicos de los equipos del usuario, gestión del software y firmware de los equipos del usuario,

monitoreo del estado y rendimiento de los equipos del usuario y diagnóstico en caso de fallos de comunicaciones.

En caso de que existiese equipo de la familia PON en el PMI, dependiendo del diseño del sistema, podrá incluir las siguientes características, además de las características del conmutador de datos y enrutador:

- PPPOE
- Ruteo estático
- Se debe de configurar y gestionar local y remotamente, además de reportar los parámetros operativos más importantes, como por ejemplo, el estado del enlace de la red de acceso.
- Monitoreo y administración vía TR069. Protocolo de administración aceptado por DSL Forum. TR069 define un conjunto de estructuras del sistema de gestión de red, incluyendo “modelo de gestión”, “interfaz interactiva” y “parámetros de gestión”. TR069 completa principalmente las siguientes funciones: configuración automática y de servicios dinámicos de los equipos del usuario, gestión del software y firmware de los equipos del usuario, monitoreo del estado y rendimiento de los equipos del usuario y diagnóstico en caso de fallos de comunicaciones.
- Interfaces E1.

b) Equipos Terminales de Fibra Óptica: En caso de tener equipos XSDL o PON en la red de acceso, se considerarán las características enlistadas en el inciso a) del PMI de este apartado, y las siguientes:
    - Administración de servicios basado en la combinación de prioridades por algoritmos SP (Strict Priority) y WRR (Weighted Round Robin).
    - Se debe de configurar y gestionar local y remotamente, además de reportar los parámetros operativos más importantes, como por ejemplo, el estado del enlace de la red de acceso.
    - Soporte a control de errores FEC.
    - Soporte a asignación de anchos de banda dinámicos DBA.

Los anchos de banda que proveerá la red de fibra óptica en el PMI, dependerán de los requerimientos calculados de acuerdo a la ecuación (1). En los puntos de agregación de enlaces, el ancho de banda se calculará de acuerdo a la ecuación (2).

IV.4.3.5 Cableado Estructurado.

El sistema de cableado estructurado está compuesto por diversos medios de transmisión como son los cables UTP y la fibra óptica además de las canalizaciones que se usan para su trasporte, áreas trabajo y diversos tipos de cuartos de equipos. El sistema de cableado estructurado permite interconectar equipos de comunicación y terminales finales de datos, voz y video. La EIA/TIA realizó una serie de recomendaciones para el cableado estructurado y actualmente son adoptadas en nuestro país.

Las series de recomendaciones de la EIA/TIA que deben cumplir las instalaciones de cableado estructurado son:

a) Serie de recomendaciones ANSI/EIA/TIA 568.
b) Serie de recomendaciones ANSI/EIA/TIA 569
c) Serie de recomendaciones ANSI/EIA/TIA 570.
d) Serie de recomendaciones ANSI/EIA/TIA 606.
e) Serie de recomendaciones ANSI/EIA/TIA 607.
f) Serie de recomendaciones ANSI/EIA/TIA 942.

- Recomendaciones: Para garantizar el funcionamiento del cableado estructurado se observarán las normas de la ANSI/EIA/TIA ya mencionadas y, adicionalmente, se seguirán los siguientes lineamientos:

1. Se utilizará la nomenclatura establecida en la norma ANSI/EIA/TIA para identificar las diversas áreas del sistema de cableado estructurado en la memoria técnica de su instalación:
   a) Instalaciones de entrada.
   b) Salas de equipos.
   c) Cableado vertical.
   d) Salas de telecomunicaciones.

e) Cableado horizontal.
f) Áreas de trabajo.

La sala de instalaciones de entrada, sala de equipos y sala de telecomunicaciones puede estar en una sola área dependiendo de las dimensiones del inmueble o el área a servir. No necesariamente deben existir todas las áreas de un sistema de cableado estructurado, esto también depende de las dimensiones del inmueble a servir.

2. Para el cableado vertical o entre cuartos de telecomunicaciones, ya sea principal o intermedios, se usará fibra óptica apegándose a las recomendaciones de las normas antes citadas. En el caso de instalaciones ya existentes con cable UTP se permitirá mantenerlo si el cableado es de cat 6.

3. La recomendación ANSI/EIA/TIA/568 permite el uso de cable cat 5 y cat 5e en adelante para el cableado horizontal. Se permitirá mantener las instalaciones existentes que usan este tipo de cable; si la instalación tiene un cable de categoría menor se tendrá que sustituir por cable cat 6 y en instalaciones nuevas se usará la categoría 6 en adelante.

4. Las canalizaciones por piso, techo, sobre muros etc., se deben apegar a las normas ANSI/EIA/TIA 569. En los lugares donde se decida utilizar tubo galvanizado solo se podrá utilizar tubo galvanizado de 20.9 mm (3/4 pulgada) como mínimo.

5. La Sala de Equipos o de Telecomunicaciones debe seguir las recomendaciones ANSI/EIA/TIA 569 además prever el crecimiento en los equipos que a futuro se irán colocando en las salas.

6. Las canalizaciones externas o backbone entre edificios de un ***campus*** puede ser subterránea, directamente enterradas, aéreas y en túneles pero deben ser con fibra óptica, con revestimiento adecuado y del tipo multimodo o monomodo dependiendo de la distancia que se requiera, para distancias menores o iguales a 2 km se utiliza fibra multimodo (MMF, por sus siglas en inglés) y para distancias

mayores a 2 km se usa fibra monomodo (SMF, por sus siglas en inglés). En caso de que el backbone sea aéreo, se debe tener en cuenta si es que así se requiere la apariencia del edificio, legislaciones aplicables, separación con los cables eléctricos además de lo que se recomienda en la norma ANSI/EIA/TIA 569. Se debe garantizar su tiempo de vida por un tiempo de **15 años mínimo** de acuerdo a la norma ANSI/TIA/EIA 568 en su última versión.

7. La infraestructura realizada para cable UTP o STP y el mismo cable debe tener un tiempo de vida mínimo de 15 años de acuerdo a la norma ANSI/TIA/EIA 568 en su última versión.

8. Se debe preferir, pero no es un requisito indispensable, que en edificios, los cuartos de telecomunicaciones, salas de equipos y la sala de instalaciones de entrada (sala donde se encuentran los equipos que conectan la red LAN hacia la red WAN), deben estar alineados verticalmente.

9. En la tabla IV.4.2 se hace la recomendación del tamaño de la sala de telecomunicaciones con base en el número de usuarios.

Tabla IV.4.2 Tamaño de la sala de telecomunicaciones con base en el número de usuarios

Relación de Número de Usuarios y Área de la Sala de Telecomunicaciones	
Número de Usuario	Área de la Sala de Telecomunicaciones
Hasta 100	14 m^2
De 101 a 400	37 m^2
De 401 a 800	74 m^2
De 801 a 1200	111 m^2

10. En el área donde exista interferencia electromagnética debido a motores, plantas de luz, etc., se deben hacer tendidos con fibra óptica y los cables de las áreas de trabajo deben ser STP aterrizados, pero preferentemente se debe evitar la instalación de equipos terminales en dichas áreas. No se deben instalar salas de comunicaciones, salas de equipos e instalaciones de entrada, salas para servidores y sistemas de almacenamiento.

11. En la puesta de cualquier tipo de canalizaciones se debe considerar el crecimiento a futuro de tal forma que sea fácil la instalación de más cable.

12. La distancia máxima permitida para el cable UTP será de 90 m, desde la sala de telecomunicaciones hasta las áreas de trabajo. En el caso de la fibra óptica en la tabla IV.4.3 se muestran las distancias de la fibra óptica.

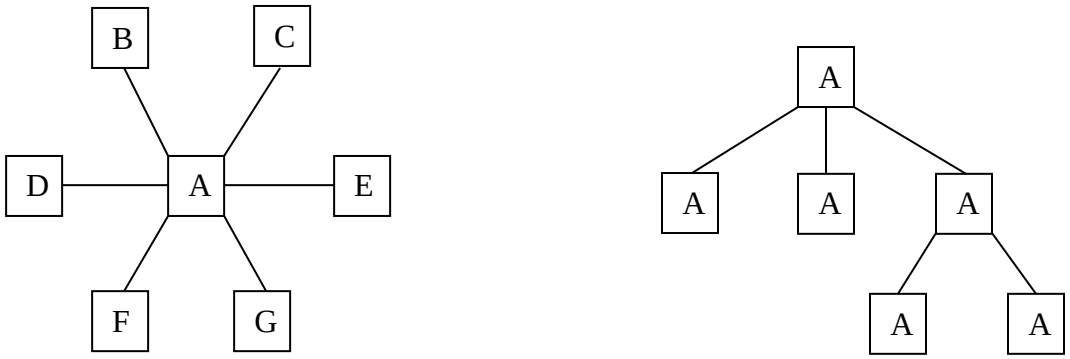
13. El sistema de cableado estructurado debe ser certificado de acuerdo a la norma TIA/EIA TSB-67, al final de su instalación.

Tabla IV.4.3 Distancia de Fibra Óptica a la Sala de Telecomunicaciones

SFP	Tipo de Fibra óptica / Longitud de Onda	Medida de la fibra óptica (µm)	Ancho de banda por km (MHz-km)	Distancia máxima de operación
100BaseFX	MMF/1310 nm	50	500	5 km
		62.5		2 km
100BaseSX	MMF/850	50	500	550 m
		62.5	200	300 m
1000BaseSX	MMF/850	62.5	160	220 m
			200	275 m
		50	400	500 m
			500	550 m
			2000	1 km
10GBaseSR	MMF/850	62.5	160	26 m
			200	33 m
		50	400	66 m
			500	82 m
			2000	300 m
10GBaseLR	SMF/1310			10 km

IV.4.3.6 Topología.

Se entenderá, para este documento, como topología la forma física en que están interconectados los equipos de telecomunicaciones con las terminales finales a través de cable UTP, STP o fibra óptica. Se empleará una topología en estrella y jerárquica en estrella con no más de dos niveles de interconexión de acuerdo a la norma ANSI/EIA/TIA 568, vea la figura IV.4.4.



a) Topología en estrella. b) Topología Jerarquía en estrella.

Figura IV.4.4. Topologías de redes de datos

De lo anterior se derivan varios casos de topología de red de acuerdo a los requerimientos de la instalación y dimensiones del área a dar servicio a través de una red LAN. En la red LAN se debe utilizar equipos de comunicaciones de tecnología tipo FastEthernet, GigaEthernet y 10GigaEthernet. En el caso de equipos de computadoras de escritorio y Lap Top´s se deben utilizar tarjetas de red del tipo FastEthernet o GigaEthernet, en el caso de teléfonos VoIP se deben utilizar tarjetas de red tipo FastEthernet o GigaEthernet.

Los escenarios a considerar son los siguientes:

a) Red en un campus. La figura IV.4.5 muestra un ejemplo de diseño en un campus.

En este caso, la figura IV.4.5 muestra una topología jerárquica. Los elementos y recomendaciones a considerar son:

- Se debe tener una Sala de Instalaciones de entrada la cual puede ser usada también como Sala de Equipos y Sala de Telecomunicaciones. En caso de usarla como Sala de Telecomunicaciones, se podrá dar servicio a equipos terminales de datos que no estén a más de 90 m y también considerando el número de usuarios a servir.

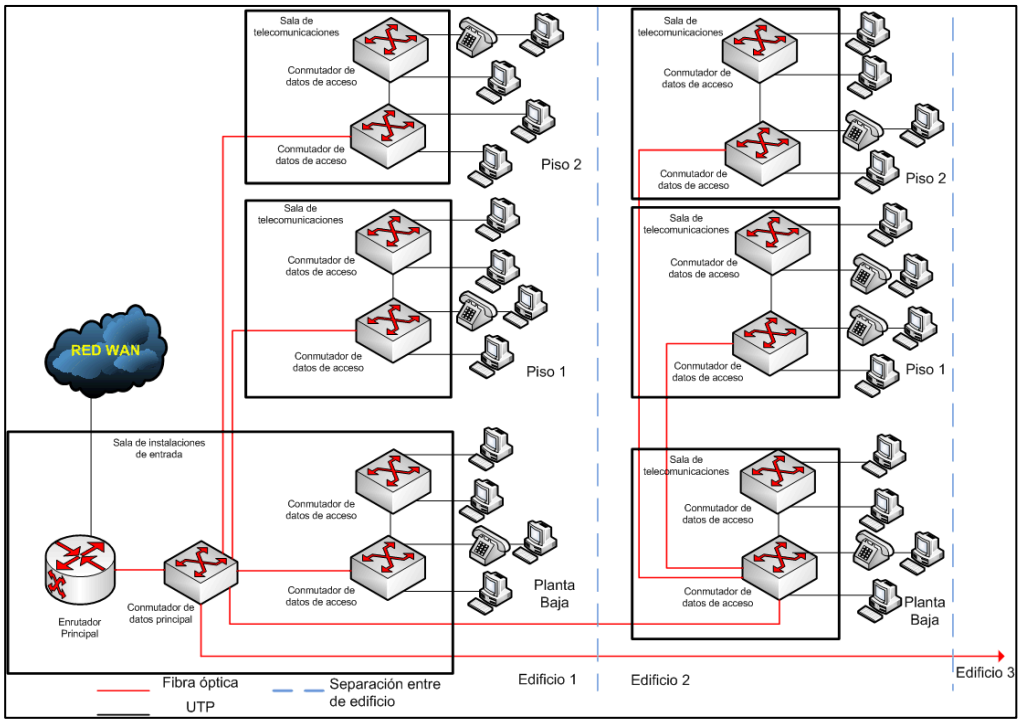


Figura IV.4.5. Topología Jerárquica en Estrella dentro de un Campus

- En la Sala de Instalaciones de entrada se permite tener la salida a la red de Internet, a la red de distribución de las cámaras y/o enlaces privados a otro centro de control.

- Las Salas de Telecomunicaciones albergan a los conmutadores de datos de acceso y de distribución. El conmutador de datos de acceso es el que se conecta con las terminales finales y recibe los enlaces de los conmutadores de

datos de distribución, y este último es el conmutador de datos de cada edificio que recibe el enlace del conmutador de datos principal y que ofrece enlaces de comunicación con los conmutadores de datos de acceso de las Salas de Telecomunicaciones de cada piso. El conmutador de datos de distribución además puede proporcionar las funciones de un conmutador de datos de acceso como se muestra en la figura IV.4.5.

- Cada piso puede tener una Sala de Telecomunicaciones o varios pisos pueden ser servidos por una sola Sala de Telecomunicaciones, esto depende del número de usuarios a servir y las distancias a cubrir de acuerdo a las recomendaciones ANSI/EIA/TIA de cableado estructurado.

- Se permite el uso de Salas de Interconexión intermedias. En la figura IV.4.5 se puede observar esto.

- La red de cámaras debe estar en uno o varios segmentos IP independiente a los segmentos IP existentes en la red LAN del Campus o del Centro de Control.

- La red LAN del Campus debe tener un plan de direccionamiento IP de tal forma que los diferentes servicios o aplicaciones estén en segmentos IP separados. Deben de estar en un segmento IP los servidores, los teléfonos IP, las PC´s de usuario, los sistemas de almacenamiento, sistemas de panel de video vigilancia, servicio telefónico de atención a emergencias, etc. Éstos a su vez pueden subdividirse en otros segmentos IP diferentes debido a la cantidad de terminales finales, a requerimientos de seguridad o administración.

- Se debe usar direccionamiento IPv4 privado, de acuerdo al direccionamiento mencionado en el RFC 1918. Las direcciones privadas, de acuerdo al RFC 1918 son:
  Para la clase A se tiene la red 10.0.0.0/8 y se pueden obtener 16,777,216 direcciones IP de nodo.

Para la clase B se tienen las redes de la 172.16.0.0/16 a 172.31.255.0/16, y cada red tiene 65,535 direcciones IP de nodo.

Para la clase C se tienen las redes de la 192.168.0.0/24 a 192.168.255.0/24, y cada red tiene 255 direcciones IP de nodo.

Para realizar el subneteo correspondiente se deben seguir los siguientes lineamientos

- Se deberán realizar subredes de las direcciones de clase A y B; en direcciones de clase C será opcional dividirla en subredes.
- De acuerdo al número de direcciones IP para equipos finales y equipos de comunicaciones se determinará la clase de direccionamiento IP a usar.
- Se podrá combinar direcciones de diferentes clases si se requiere.
- Se recomienda tener una subred IP por departamento siempre que el departamento tenga alrededor 120 usuarios, en caso contrario se dividirá el departamento en subredes no mayores de 120 usuarios.
- La granja de Servidores VMS y aplicaciones de uso exclusivo del Centro de Control deberán estar en una subred IP así como el Sistema de Almacenamiento y en otra subred IP los Servidores de Actualizaciones. Se puede tener el Sistema de Almacenamiento en la subred donde está el Servidor VMS y Servidores de aplicaciones de uso exclusivo del Centro de Control si se tiene poco espacio o si es para hacer más entendible la configuración.
- El direccionamiento usado en la administración deberá estar en una subred.

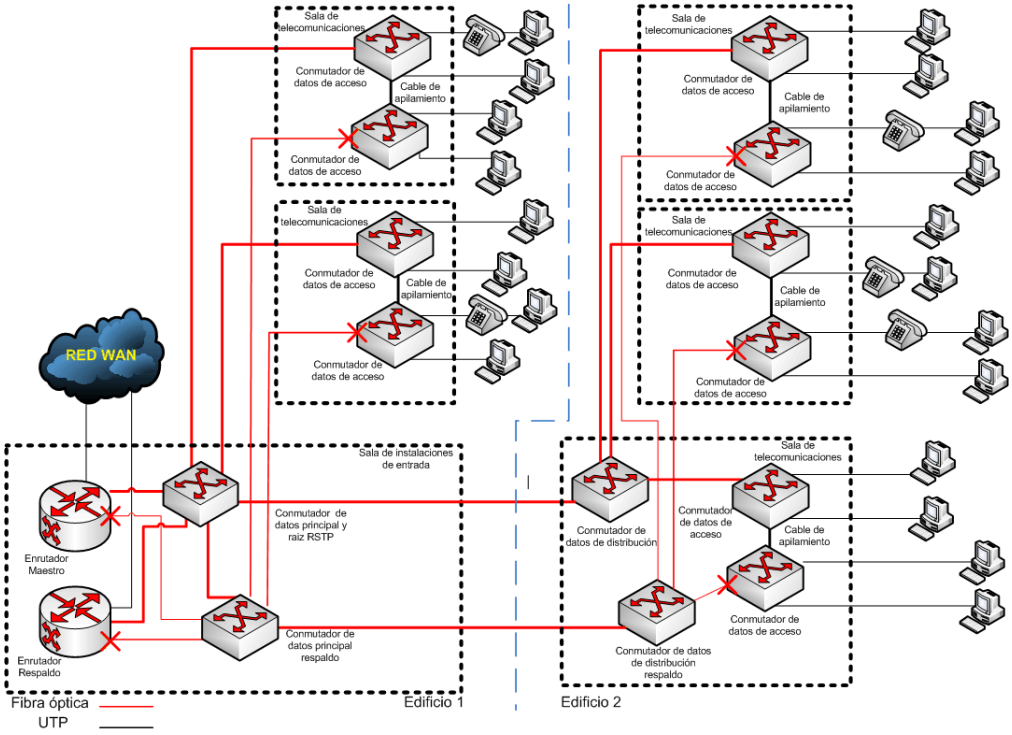
En caso de usar direccionamiento IPv6, se utilizarán direcciones Locales Únicas (ULA Unique Local Addres) definidas en el RFC 4193 y las mismas consideraciones mencionadas para IPv4. Las direcciones IPv6 Locales Únicas son de uso local como las direcciones IP v4 privadas. Siendo una dirección IPv6 de 128 bits se tiene el siguiente formato:

- Empiezan con el valor FC00::/7
- El octavo bit vale siempre 1

- Los siguientes 40 bits es un identificador global que será único para cada Centro de Control y de acuerdo al RFC 4193 se asignará de manera aleatoria.
- Los siguientes 16 bits es el número de subred y este puede dado de forma secuencial o con cualquier otro método.
- Los últimos 64 bits está formado por la dirección MAC de la interfaz en formato EUI-64

- Cada segmento IP debe implementarse con el uso de la norma IEEE 802.1q (VLAN); además se debe utilizar una VLAN diferente para cada uno de los servicios (video, voz, administración, etc).
- Los servidores deben estar todos ubicados en un área dentro de una de las salas, la cual llevará el nombre de Granja de Servidores. Los servidores de esta granja deben estar en su propio segmento IP. Esto puede cambiar por razones de seguridad.
- Todos los sistemas de almacenamiento también deben estar ubicados juntos en una de las salas. Esto puede cambiar por razones de seguridad.
- Opcionalmente se permite implementar redundancia en los conmutadores de voz y enrutadores además del cableado como lo muestra la figura IV.4.6.

Figura IV.4.6. Redundancia de Conmutadores de datos, enrutadores y cableado


Sala de telecomunicaciones
Conmutador de datos de acceso
Cable de apilamiento
Conmutador de datos de acceso
RED WAN
Sala de instalaciones de entrada
Conmutador de datos principal y raiz RSTP
Enrutador Maestro
Enrutador Respaldo
Conmutador de datos principal respaldo
Conmutador de datos de distribución
Conmutador de datos de distribución respaldo
Fibra óptica
UTP
Edificio 1
Edificio 2

Observando la figura IV.4.6, los conmutadores de datos principales, conmutadores de distribución y enrutadores tienen respaldo así como los enlaces entre dichos equipos. Los conmutadores de acceso no se respaldan y están conectados de forma apilada con cables y puertos para este propósito.

Los enrutadores respaldan la puerta de enlace que usan las terminales finales y para este fin se utiliza el Protocolo de Redundancia de Enrutador Virtual (VRRP) explicado en el apartado IV.4.8 inciso a) titulado “Protocolos de capa de red”.

Los conmutadores de datos y los enlaces redundantes funcionan de acuerdo al protocolo 802.1w conocido como Protocolo Rápido de Árbol de Expansión (RSTP). Sin este protocolo, al conectar una topología como muestra la figura IV.4.6 provocaría que la información viajara en la red de forma circular ya que los enlaces redundantes toman esta forma al conectar varios conmutadores de datos; sí esto llegara a suceder el ancho de banda lo consumiría la información que viaja de forma circular en la red. El RSTP detecta estos caminos circulares y para poderlos abrir, el RSTP elige puertos para que operativamente dejen de funcionar es decir se dan de baja. En caso de que un conmutador o enlace se dañe o apague de forma accidental o se desconecte los puertos volverán a activarse (se dan de alta) de esta forma abra redundancia en caso de un fallo en un enlace o conmutador de datos.

Para el funcionamiento operativo del RSTP, se tiene un conmutador de datos denominado raíz. Se debe configurar el conmutador de datos principal de tal forma que sea la raíz y si éste llegara a fallar entonces el conmutador de datos de respaldo sería raíz. Todos los equipos de comunicación con el protocolo RSTP tienen activo un enlace con el fin de mantener una ruta hacia la raíz, esto se muestra en la figura IV.4.6 con los enlaces rojos gruesos y las líneas que simbolizan el cable de apilamiento también gruesa, este conjunto de cables son los que se utilizarán para la comunicación de datos de usuario. Los demás enlaces serán los redundantes que se activarán al momento de fallar un dispositivo de comunicación o un cable; el protocolo RSTP dará de baja uno de

los puertos de estos enlaces para que no sea funcional y esto se muestra con un tache en la figura IV.4.6.

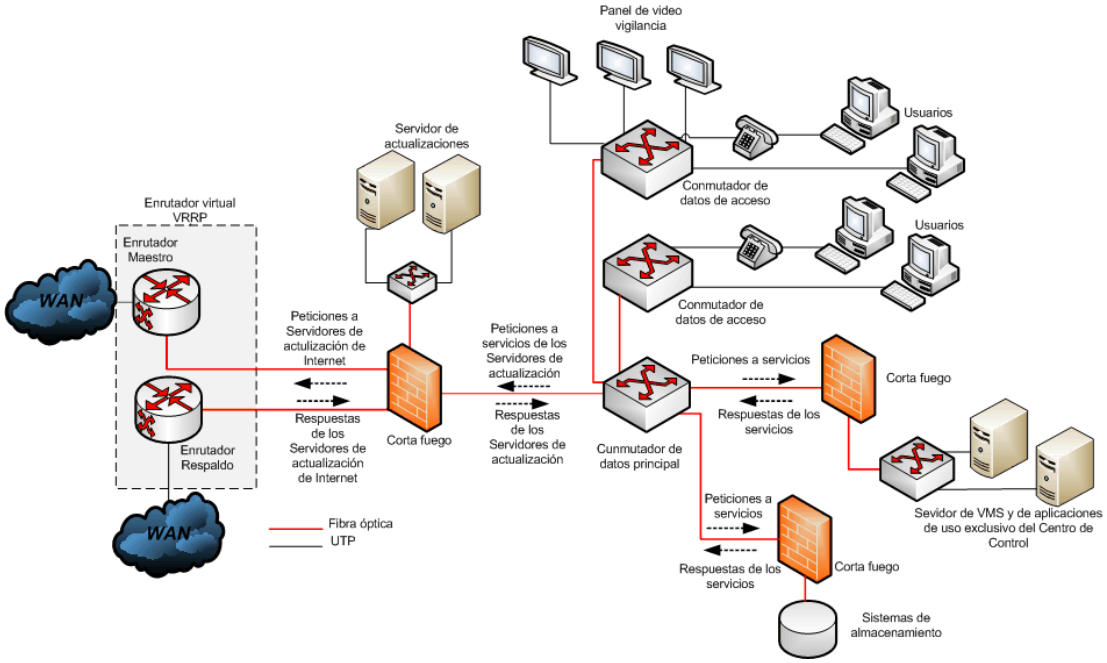
- Los Servidores y Sistemas de Almacenamiento deben estar protegidos con equipos de seguridad como son: Sistema de Prevención de Intrusos (IPS), Antivirus, Antispam, Corta Fuegos, Filtro de Páginas Web, etc. Se debe tener por lo menos la restricción de acceso por medio del Corta Fuegos y Antivirus.

  La figura IV.4.7 ejemplifica la posición de los Corta Fuegos y muestra el flujo de peticiones y respuestas para acceder a los diferentes servicios a través de éste. Se contempla que para proteger a los Servidores del Sistema de Administración de Video (VMS) u otros servicios de uso exclusivo del Centro de Control sea a través de un Corta Fuego colocado después del conmutador de datos principal del Centro de Control, el Sistema de Almacenamiento con otro Corta Fuego también colocado después del conmutador de datos principal y los servidores de actualización sea con otro Corta Fuego colocado entre los enrutadores y el conmutador de datos principal. Los Servidores de Actualización son para que a través de él se actualicen equipos de cómputo o equipo de comunicaciones bajando parches y programas de actualizaciones.

  La forma de trabajar del Corta Fuego será permitir sólo los puertos utilizables por las aplicaciones del Centro de control y bloquear todos los demás. Se debe verificar qué puertos usan las aplicaciones válidas del Centro de Control para abrirlos en el Corta Fuego, como es el caso de las actualizaciones de los antivirus, pero también hay puertos bien conocidos y en caso de que se estén utilizado para ser alcanzables a través de un Corta Fuego, se deben permitir. Los siguientes puertos son de aplicaciones bien conocidas:
  - SSH puerto 22
  - FTP puerto 20 y 21 (se recomienda abrir este puerto solo al momento de usarse)
  - TFTP puerto 69 (se recomienda abrir este puerto solo al momento de usarse)
  - Bootstrap/DHCP servidor puerto 67

- Bootstrap/DHCP cliente puerto 68
- DHCPv6 servidor puerto 547
- DHCPv6 cliente puertdo 546
- IPsec puerto 1293
- IPsec NAT trasversal (RFC 3947) puerto 4500
- TACACS puerto 49
- DNS puerto 53
- SNMP puerto 161 y 162
- https puerto 443
- Syslog puerto 514
- Syslog sobre TLS puerto 6514
- RIP puerto 520
- ICMP/ping/tracer-route protocolo 1
- SNTP/NTP puerto 123
- RIPng puerto 521
- RTSP (protocolo de video en tiempo real) puerto 554
- RADIUS puerto 1812 y 1813
- RADIUS seguro 3799 y 2083
- IMAP puerto 143/220/993
- POP3S puerto 995
- SMTPS puerto 465
- IKE/ISAKMP puerto 500

Figura IV.4.7. Puntos a Proteger por un Corta fuego



- Los enlaces entre el conmutador de datos principal y los conmutadores de datos de distribución, y los enlaces entre conmutadores de datos de distribución con los conmutadores de datos de acceso, deben de ser de fibra óptica a 1 Gbps por lo menos para instalaciones nuevas, pero se recomienda el usa de 10GEthernet. Las instalaciones existentes con cobre podrán mantenerse sí los enlaces entre los dispositivos mencionados están a una velocidad de 1 Gbps, por lo menos. Estos enlaces se deben implementar con SFP.

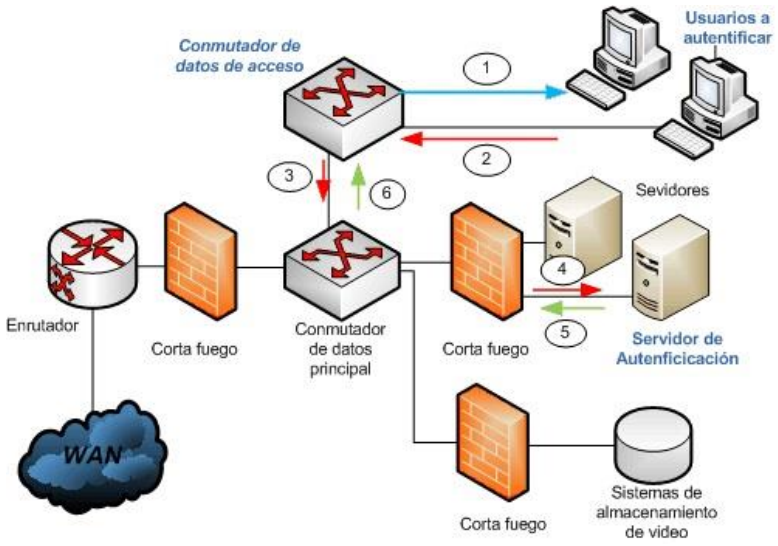
- Cuando se tengan varios conmutadores de datos de acceso en una Sala de Telecomunicaciones, se debe realizar una conexión tipo stack entre éstos.

- Se permite el uso de gabinetes de red que cumplan con la normatividad EIA-310-E como mínimo para sustituir la Sala de Telecomunicaciones, solamente para montar equipos de conectividad como conmutador de datos o enrutadores. No se permite instalación de monitores, servidores u otro tipo de equipo terminal y solo si se va a dar servicio al piso donde se va instalar.

- El conmutador de voz IP y el panel de video vigilancia deberán incluir software para su administración y gestión de sus funciones. Dicho software, para el panel de video vigilancia y para el conmutador, deben utilizar protocolos abiertos de comunicación, administración y gestión, de tal forma que se puedan usar teléfonos de diversas marcas así como monitores o equipo de control de grabación para video.

- Se debe considerar una solución de autentificación de las Computadoras Personales (PC); puede estar basada en autentificación por MAC, contraseñas, etc. Para esta solución se utilizará el protocolo 802.1x. La figura IV.4.8 muestra los elementos que se requieren considerar.

Figura IV.4.8 Arquitectura 802.1x para Autentificación



Los elementos de la arquitectura son: los usuarios a autentificar, el conmutador de datos de acceso con 802.1x y un Servidor de Autentificación como RADIUS o TACACS. Los usuarios a autentificar son los dispositivos que se van autentificar en la red para permitirles el acceso y uso de ésta, como pueden ser PC´s o cualquier tipo de terminales finales. Al momento de ser prendidas o al querer conectarse con la red de datos, deberán

ser detectadas por el conmutador de datos de acceso y solicitará el conmutador de datos a la PC sus credenciales (línea 1 de la figura IV.4.8).

La PC envía dichas credenciales (línea 2), el conmutador de datos se las manda al Servidor de Autentificación (línea 3 y 4), el Servidor de Autentificación las revisa y manda un respuesta al conmutador de datos de acceso (línea 5 y 6). Sí la respuesta de la solicitud de autentificación es exitosa, el conmutador de acceso permite a la PC conectarse a la red, en caso contrario bloqueará el puerto.

- Políticas de administración y seguridad de los equipos.
    - Se deben deshabilitar las cuentas que vienen pre configuradas por defecto en los equipos de comunicaciones y crear cuentas de usuario con los mismos privilegios.
    - La administración de cada componente debe hacerse únicamente a través de las cuentas administrativas definidas para cada componente.
    - La contraseña de cada cuenta administrativa debe apegarse a la política de contraseñas.
    - Todos los equipos deben tener contraseñas diferentes.
    - Se debe establecer una política de creación de contraseñas por los administradores de la red que defina longitud de la contraseña, caracteres válidos y periodo de cambio de la misma
    - Los servicios para la conexión y administración de los componentes que no cifren los canales de comunicación se deben deshabilitar por considerarse inseguros ante un ataque de Sniffing en la red.
    - Se debe tener una VLAN para la administración.
    - Se debe restringir el acceso a los componentes únicamente a un determinad número de direcciones IP y/o segmentos de red
    - Se debe establecer un control de cambios de las contraseñas
    - Se debe establecer un control de cambios para la aplicación de las actualizaciones de los firmware de los equipos que sean aprobadas, el cual debe considerar como mínimo lo siguiente:
        - Justificación de la instalación.

- Resultado de la evaluación de la actualización realizada en ambientes de pruebas.
- Plan para la aplicación de la actualización.
- Fecha de la actualización.
- Respaldo de las configuraciones y
- Procedimiento de regreso en caso de que la actualización genere problemas en el ambiente productivo.
- Autorización del cambio por la dirección responsable.

  - Se deben desactivar protocolos que no se usen.
  - Contar con diagramas de la ubicación física de los equipos de comunicaciones del Centro de Control y estar etiquetados para su fácil identificación.
  - Contar con un inventario actualizado donde se identifiquen las conexiones entre los conmutadores de datos y los demás equipos de red.

- Se debe solicitar que la memoria técnica incluya pruebas de transferencia de diversos MTU, pruebas de retardo y pruebas de pérdida de paquete, en conformidad con el RFC 2544.

b) Red LAN en un edificio

La red LAN dentro de un edificio es un caso particular del punto anterior, incluso la figura representativa de este caso es la IV.4.7 del caso anterior. Se observa en dicha figura que es una topología jerárquica en estrella y se sigue utilizando la tecnología FastEthernet, GigaEthernet y 10GigaEthernet. Se aplican las mismas recomendaciones dadas para el caso anterior con las siguientes diferencias:

- Se suprime el conmutador de datos de distribución, el roll de éste lo toma el conmutador de datos principal. Se permite el uso del conmutador de datos de distribución para casos justificables.
- Se recomienda tener Salas de Telecomunicaciones para tener mejor administración de los usuarios, pero sí se permite tener una Sala de Telecomunicaciones para todo el inmueble mientras cumpla con las normas ANSI/EIA/TIA para cableado estructurado mencionadas.

IV.4.3.7 Protocolos de la IEEE 802 y de la IETF para la Red LAN.

Los protocolos que a continuación se describen están normalizados por la IEEE y la IETF y tienen una gran aceptación en la industria de las telecomunicaciones. Normalmente son implementadas por la gran mayoría de fabricantes de equipos de comunicaciones como son fabricantes de conmutador de datos, enrutadores, access point, etc.

De la siguiente lista de protocolos deberán de escogerse los que satisfagan los requerimientos de la red LAN. Se comentarán los protocolos válidos y de mayor uso en la LAN, si existiera un requerimiento que no lo resuelve alguno de los protocolos listados, se deberá buscar un protocolo abierto recomendado por una organización nacional o internacional.

Los protocolos se dividen en protocolos de capa de red o capa 3 del modelo de interconexión de sistemas abiertos (OSI, por sus siglas en inglés), protocolos de capa de enlace de datos o capa 2 del modelo OSI y protocolos de la capa de aplicación del modelo de referencia TCP/IP. Dependiendo de las necesidades de cada uno de los puntos de la red LAN se determina qué equipo debe soportar un protocolo dado.

a) Protocolos de capa de red

- Soporte a protocolos IPv4 e IPv6: Debe cumplir con los RFC 791, 1349 y 6864 para IPv4; y para el caso de IPv6 se deben cumplir los RFC 2460 y RFC 5722.

- Direcciones primarias y/o secundarias por interfaz o VLAN (802.1q): Los equipos con capacidades de enrutamiento deben poder soportar el uso de direcciones IP en sus interfaces o en VLAN por puerto. Es opcional que además de poder asignar una primera dirección IP, se pueda asignar direcciones IP secundarias extra, esto depende del diseño o requerimientos.

- Rutas estáticas: Los equipos con capacidades de enrutamiento deben tener la posibilidad de configurar manualmente rutas para llenar su tabla de enrutamiento.

- Protocolo de ruteo dinámico RIPv2 y OSPF para IPv4 e IPv6. El protocolo de ruteo dinámico RIP debe cumplir con lo especificado en el RFC 2453 y el RFC 2080 y es recomendable para redes pequeñas cuando subredes están a no más de 15 enrutadores de separación. Para el caso de OSPF debe cumplir con el RFC 2328 y el RFC 5340 y se recomienda cuando el número de subredes supera a las limitantes de RIP v2.

- VRRP: Debe cumplir con el RFC 5798; este protocolo da la posibilidad de respaldar las puertas de enlace de una red o subred IP, a través de la implementación de un segundo enrutador. Con apoyo de un enrutador de respaldo, se configura un enrutador virtual donde se encuentre el enrutador primario y el de respaldo. El enrutador virtual tiene una dirección IP que será la puerta de enlace de todos los dispositivos de red. Mientras el enrutador primario esté activo, atenderá las solicitudes hacia la puerta de enlace haciendo su labor de enrutamiento, mientras el de respaldo monitorea el estado del enrutador primario. En el momento en que el enrutador primario falle, lo detectará el enrutador de respaldo tomando su lugar.

- DHCP: Debe cumplir con el RFC 2131 y el RFC 3046. Un equipo con capacidades de enrutamiento puede ser un servidor DHCP, cliente DHCP y/o DHCP de reenvío. El servidor DHCP nos permite asignar direcciones IP de host a los clientes DHCP. El cliente DHCP en un enrutador permite que a sus interfaces se le asigne una dirección IP por medio de un servidor DHCP. El DHCP de reenvío manda las peticiones de clientes DHCP al servidor DHCP.

- IGMP: Debe cumplir con el RFC 2236. Este protocolo permite que todos los grupos multicast sean anunciados a los protocolos de ruteo multicast, en el caso de los enrutadores, o sean identificados sus miembros en los puertos de un conmutador de datos.

- PIM-S-M: Debe cumplir con el RFC 7761. Permite el ruteo multicast.

- DVMRP. Debe cumplir con los RFC 1075 y 2715. Permite el enrutamiento con direcciones IP multicast.

- NAT Estático o Básico: Deberá cumplir con el RFC 2663. Permite que un servidor o servicio dentro de una red privada, pueda ser accesible desde otra red donde el direccionamiento del primero no es válido.

- NAPT: Deberá cumplir con el RFC 3022. Este protocolo permite que una red IP con un direccionamiento no válido en otra red IP, pueda comunicarse con esta última. Por ejemplo suponiendo una red IP de un centro de control cuyo direccionamiento se realizó con direcciones IP privadas y dicho centro quiere que ciertas terminales de red puedan tener acceso a Internet pero su direccionamiento privado no es válido; NAPT le permitirá la comunicación entre la red IP del centro y la red de Internet. Cabe mencionar que no se podrá dar la comunicación en sentido contrario.

- SNTP: Deberá cumplir con el RFC 4330. Usado cuando se requiere que los equipos sincronicen su reloj tomándolo de un servidor de tiempo.

- VPN IPSec: Deberá cumplir con el RFC 4301. Usado en la creación de accesos remotos, sitio a sitio o de sitio a múltiples sitios de forma segura, normalmente este tipo de accesos se le llama túnel.
- VPN GRE: Deberá cumplir con el RFC 2784. Usado en la creación de accesos sitio a sitio o de sitio a múltiples sitios de forma segura, normalmente este tipo de accesos se le llama túnel.

- QoS DSCP/Precedencia IP: Protocolo que utiliza el marcado de paquetes IP en el campo TOS del encabezado que permite darle un tratamiento para priorizar tramas.

b) Protocolos de capa de enlace de datos.

Los equipos que tengan funcionalidad:

- IEEE 802.1x: Es una norma para la autentificación de usuarios basado en puertos.
- IEEE 802.1q: Norma que describe el funcionamiento, formatos de paquetes y parámetros de las VLAN.
- GVRP: Definido en la norma IEEE 802.1q y 802.1ak. Permite el descubrimiento de VLAN´s en forma dinámica.
- IEEE 802.1p: Norma que define un método para marcar y dar tratamiento a tramas para fines de calidad de servicio.
- IEEE 802.1w: Norma que describe el funcionamiento del Protocolo Spanning Tree, utilizado para dar redundancia en los enlaces en una red de área local.
- IEEE 802.1s: Norma que describe el funcionamiento del Protocolo Múltiple Spanning Tree, utilizado para dar redundancia en enlaces de una red de área local tomando encuentra las VLAN existentes.
- IEEE 802.1t: Norma que establece extensiones del protocolo 802.1w y 802.1s, por lo que en caso de utilizar estas dos últimas normas se deberá incluir ésta.
- IEEE 802.3ad: Norma que describe un método para crear un grupo de puertos físico con el fin de sumar anchos de banda. Este grupo de puertos físicos se conectan del conmutador de datos a otro conmutador de datos o del conmutador de datos a un servidor para aumentar la velocidad de transmisión de información.
- IEEE 802.3x: Norma que establece un mecanismo de control de flujo para así evitar congestionamientos.
- IEEE 802.3af: Norma que regula la alimentación que puede recibir o dar un equipo a través de los puertos de Ethernet.
- IEEE 802.3az: Norma que regula el ahorro de energía.
- IEEE 802.1Qau: Norma que establece mecanismos para evitar la congestión en redes de alto uso de ancho de banda.

c) Protocolos de la capa de aplicaciones.

No se permite el uso de Telnet y HTTP, en caso de que el equipo tenga implementado estos protocolos, deberán ser deshabilitados. Las aplicaciones aquí recomendadas son para fines de administración y actualización de equipo.

- Radius: Permite la autentificación de los usuarios al ingresar a la red de datos.

- SNMPv2c/v3: Protocolo que permite el monitoreo de dispositivos de red.
- SSHv2: Protocolo que permite el acceso remoto a un equipo de red de forma segura vía línea de comandos.
- FTP/TFTP Cliente: Protocolos que permiten la transferencia de archivos. Usual para actualizar firmware o archivos de configuraciones o respaldarlos.
- Syslog: Protocolo que permite el almacenamiento de mensajes de eventos en servidores remotos.
- RMON: Protocolo que da un conjunto de variables o MIB´s para el monitoreo de red así como un protocolo para la consulta de estos MIB´s.
- HTTPS: Protocolo basado en hipertexto para el monitoreo de un dispositivo de red.

Se han abordado y detallado los elementos que componen un punto de monitoreo inteligente y la manera en que pueden darse las telecomunicaciones desde este punto con un centro de control, por consecuencia ahora definiremos cada uno de los elementos que componen a este centro y posteriormente hablaremos de la administración del mismo.

IV.5 Centro de Control.

IV.5.1 Resumen.

El Centro de Control de un Sistema de Video Vigilancia es el núcleo de todo el sistema. Permite recibir y almacenar todos los datos captados en los Puntos de Monitoreo Inteligente (PMI) que son enviados usando protocolos seguros a través de algún medio de comunicación.

Para que la información fluya adecuadamente de los PMI al Centro de Control, es indispensable realizar estudios adicionales sobre la diversidad de medios de comunicación disponibles entre ambos puntos (pasando, si es necesario, por puntos intermedios) o proponer nuevos medios de enlace que cumplan con este objetivo. Para esta tarea, se necesita de una investigación a fondo de los requerimientos de comunicación, de modo que se cumpla con las necesidades planteadas.

Igualmente, es necesario destacar que este apartado de la Norma refiere a la seguridad del sistema. El resguardo de la información, así como los protocolos seguros de transmisión de los datos, son temas que preocupan a la sociedad civil y que, como responsables de este documento, debemos atender con atención a los estándares nacionales e internacionales.

Al definir claramente el medio de enlace y las políticas de seguridad, la información puede llegar sin inconvenientes al Centro de Control del Sistema de Video Vigilancia, con la garantía de que los derechos de la ciudadanía están siendo resguardados. El uso de mecanismos obligatorios como cortafuegos (*firewalls*), entre otros, busca proteger los datos de cualquier tipo de intrusión o ataque informático.

En resumen, el Centro de Control es el encargado de procesar la información que se recibe de las calles a través de los PMI. Los recursos técnicos a su disposición deben ser aprovechados en forma eficiente. La eficacia de los Sistemas de Video Vigilancia debe ser medida con base a métricas definidas en esta Norma Técnica con base a las mejores prácticas.

IV.5.2 Glosario

Para contextualizar la información en el ámbito de la presente Norma, se presenta a continuación un glosario de términos y definiciones relacionadas.

- CC: Centro de Control para un Sistema de Video Vigilancia
- SVV: Sistema de Video Vigilancia
- SGSI: Sistema de Gestión de la Seguridad de la Información
- Video-Wall (Pared de video): Arreglo matricial de pantallas que extiende las capacidades de visualización para una organización
- C4 (Centros de Control, Comando, Cómputo y Comunicaciones): Un centro de control y comando proporciona servicios de seguridad pública, atención y despacho de emergencias de manera oportuna mediante equipo y sistemas tecnológicos que permiten la oportuna toma de decisiones y correcta ejecución de acciones para la pronta y eficaz respuesta a la población.
- TI: Tecnologías de la Información
- AWUT: (Average Wrap Up Time), es el tiempo en que un operador no está disponible después de terminar una llamada.
- Erlang: Modelo matemático de tráfico para obtener el número de operadores y de líneas necesarias para un sistema para la atención de llamadas
- Video de flujo Diario: hace referencia al video que es recibido en tiempo real por las videocámaras del Sistema de Videovigilancia.
- Video de Incidentes: son los videos que se derivan del flujo diario donde el operador de videovigilancia detecte algún incidente de acuerdo con el Catálogo Nacional de Incidentes de Emergencia. Así mismo, cuando originado de algún reporte de incidente proveniente de una llamada de emergencia, uno o varios operadores de videovigilancia puedan dar seguimiento con alguna de las videocámaras.
- Video de Evidencia: se consideran a todos aquellos videos que se vean involucrados en una Solicitud de Grabación.
- Video de Reserva en Sitio: son aquellas grabaciones almacenadas en la misma cámara, para aquellas que tienen la posibilidad de contar con almacenamiento en la misma.

- AES: Advanced Encryption Standard (AES), también conocido como Rijndael, es un esquema de cifrado por bloques adoptado como un estándar por el gobierno de los Estados Unidos. Usa claves de al menos 128 bits.
- Redundancia: es la duplicación de críticos componentes o funciones de un sistema con la intención de aumentar la fiabilidad del sistema , por lo general en forma de una copia de seguridad o a prueba de fallos. Se presenta como una solución a los problemas de protección y confiabilidad.
- DBMS: (Data Base Management System), es un sistema de administración de bases de datos
- RAID: (Redundant Array of Independent Disks), es un sistema de almacenamiento de datos en tiempo real que utiliza múltiples unidades de almacenamiento de datos entre los que se distribuyen o replican los datos. Dependiendo del grado de redundancia se especifican varios niveles.
- SAS: (Serial Attached SCSI) es una interfaz de transferencia de datos en serie, sucesor del Small Computer System Interface (SCSI) paralelo, aunque sigue utilizando comandos SCSI para interaccionar con los dispositivos SAS. Aumenta la velocidad y permite la conexión y desconexión de forma rápida. Además, el conector es similar que en la interfaz Serial ATA (SATA) y permite utilizar estos discos duros, para aplicaciones con menos necesidad de velocidad, ahorrando costes. Por lo tanto, los discos SATA pueden ser utilizados por controladoras SAS pero no a la inversa, una controladora SATA no reconoce discos SAS.
- TIER: El TIER de un Data Center es una clasificación ideada por el Uptime Institute que se plasmó en el estándar ANSI/TIA-942 y que básicamente establece 4 categorías, en función del nivel de redundancia de los componentes que soportan el Datacenter.
- RAM: (Random Access Memory), es la memoria principal de una computadora
- KB: Kilobyte, equivale a 10 elevado a la 3 bytes
- MB: Megabyte, equivale a 10 elevado a la 6 bytes
- GB: Gigabyte, equivale a 10 elevado a la 9 bytes
- SSD: (Solid-State Drive), es un tipo de dispositivo de almacenamiento de datos que utiliza memoria no volátil, como la memoria flash, para almacenar datos, en

lugar de los platos o discos magnéticos de las unidades de discos duros (HDD). Es el más rápido sistema de almacenamiento de alta densidad

- HBA: (Host Bus Adapter), es un dispositivo de hardware que proporciona la interfaz para E/S entre un host y un sistema de almacenamiento. RealTime Server usa un adaptador de bus host para lograr conectividad de Fibre Channel a la SAN del sitio. Es una interfaz entre un servidor o un bus de estación de trabajo y una red de Fibre Channel.
- NAS: (Network Attached Storage), es una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un computador (servidor) con computadoras personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un sistema operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.
- GPU: (Graphics Processor Unit), es un coprocesador dedicado al procesamiento de gráficos u operaciones de coma flotante, para aligerar la carga de trabajo del procesador central en aplicaciones como los videojuegos o aplicaciones 3D interactivas.
- NVRAM: (Non-volatile random access memory), es un tipo de memoria de acceso aleatorio que, como su nombre indica, no pierde la información almacenada al cortar la alimentación eléctrica.
- ECC: (Error-Correcting Code), es una tecnología que sirve para garantizar la integridad de los datos en una memoria.
- QUERTY: Se refiere a la distribución de teclas en un teclado, es la distribución de teclado más común. Fue diseñado y patentado por Christopher Sholes en 1868 y vendido a Remington en 1873. Su nombre proviene de las primeras seis letras de su fila superior de teclas.
- CAD: (Computer Aided Dispatch), es un Sistema de Despacho o Atención asistido por un Sistema de Cómputo.
- GIS: (Geographic Information System), es un conjunto de herramientas que integra y relaciona diversos componentes (usuarios, hardware, software, procesos) que permiten la organización, almacenamiento, manipulación, análisis y modelización de grandes cantidades de datos procedentes del mundo real que están vinculados a una referencia espacial, facilitando la incorporación de aspectos sociales-

culturales, económicos y ambientales que conducen a la toma de decisiones de una manera más eficaz.

- AVL: (Automatic Vehicle Location), se refiere al rastreo de vehículos realizada de manera automatizada
- FPS: (Frame Per Second), se refiere a la cantidad de fotogramas grabados por segundo para un video
- Sala de crisis: son espacios que permiten la colaboración cercana de diferentes actores encargados de la respuesta a las situaciones de emergencia, permitiendo una mayor coordinación, mejores los flujos de información y toma de decisiones.
- Cámaras de alta definición: Este tipo de cámaras ofrece resoluciones superiores a las obtenidas con cámaras analógicas.
- Cámaras Día/Noche: Las cámaras de seguridad que tienen esta especificación poseen una sensibilidad a la luz de por lo menos 0.01 lux lo que las hace efectivas para monitoreo en lugares con muy poca luz. En estas condiciones, estas cámaras cambian su configuración de color a blanco y negro automáticamente, logrando una sensibilidad a la luz mucho mayor.
- Compresión: Métodos que permiten disminuir el tamaño inicial de una imagen digitalizada aplicando algoritmos que eliminan información redundante a expensas de la calidad de la imagen final.
- Descompresión: Transformar la información comprimida digitalmente y reproducir las imágenes de video normal.
- Cámaras PTZ (Pan-Tilt-Zoom): En estas cámaras se encuentran instalados motores que permiten el control remoto para el apuntamiento de la cámara tanto vertical (elevación) como horizontalmente (azimut), esta característica permite lograr la inspección de una zona en 360°, también cuentan con la capacidad de realizar acercamientos (zoom) para obtener detalles de algún punto de interés.
- Cámaras IP: Mediante las cámaras IP se obtienen mayores resoluciones que con cámaras analógicas convencionales. Por otro lado el ancho de banda utilizado es menor debido a la compresión de video, también permiten realizar el monitoreo, no solo del video transmitido, sino que también permiten conocer su estado.

- Grabador de video digital DVR: Almacena las imágenes tomadas de canales distintos de grabación. En algunos casos cuentan con detectores de movimiento, entradas de alarma y sistema de conexión remota.
- Pixel: Es la unidad usada para expresar la resolución.
- Protocolo: Lenguaje de comunicación estandarizado para diferentes dispositivos
- Resolución: Es una medida del grado de detalle de una imagen digital, se puede especificar como el número de columnas de píxeles (horizontal) por el número de filas de píxeles (vertical).
- Trama (Frame): Se refiere al número de cuadros por segundo (fps) al cual se muestra o graba el video. Las transmisiones de TV convencionales son a 30 fps, ya que esta tasa es considerada como video en tiempo real.
- Sistema de alimentación ininterrumpida (UPS): es un dispositivo que cuenta con baterías capaces de almacenar energía eléctrica para proporcionar alimentación a los equipos conectados a éste durante un corte de energía eléctrica de la red pública.
- Zoom: El zoom se encuentra ligado al lente de la cámara, esta característica permite acercar la toma para obtener mayores detalles de un objeto específico en la escena bajo inspección.
- PPI (Pixels per Inch): Es una unidad de medida de resolución de fotos o dispositivos digitales como, por ejemplo, impresoras y cámaras digitales, se refiere al número de píxeles distintos que tiene una imagen por unidad de longitud, es decir, la densidad de éstos en la imagen.
- Shape Files (SHP): Son archivos vectoriales, compuestos por entidades de tipo punto, línea y área. Un archivo Shape se compone a su vez de tres archivos con extensión .SHX .SHP y .DBF en los cuales se almacena información geométrica y alfanumérica. Estos archivos pueden utilizarse con paquetes que manejen información vectorial para sistemas de información geográfica.
- KMZ (Keyhole Markup Zip): Estos archivos almacenan localizaciones en el mapa visibles en Google y permiten empaquetar varios archivos juntos y comprimen el contenido para que sean más fáciles de descargar. Esto te permite unir imágenes al archivo KML.

- KML (Keyhole Markup Language): Es un fichero que contiene datos geográficos. Mediante estos archivos se pueden situar en un mapa distintos lugares que estén relacionados. Han sido desarrollados para ser manejados con el programa Google Earth, pero también se pueden utilizar con la aplicación de Google Maps.
- GDB (Geodatabase): Es una colección de datasets geográficos de varios tipos contenida en una carpeta de sistema de archivos común, una base de datos de Microsoft Access o una base de datos relacional multiusuario DBMS. Almacena físicamente información geográfica.
- ArcInfo: Es un software de tipo escritorio con funcionalidad completa (vectorial y raster) para cualquier tarea dentro de un Sistema de Información Geográfica (SIG) profesional.
- ArcGIS: Comprende una serie de aplicaciones, que utilizadas en conjunto, permiten realizar funciones que alimentan y administran un sistema de información geográfica (SIG), desde creación de mapas, manejo y análisis de información, edición de datos, metadatos y publicación de mapas en la Internet.
- ArcSDE (Motor de base de datos espacial): Sirve para acceder y administrar datos geoespaciales dentro de las bases de datos relacionales. La tecnología de ArcSDE admite la lectura y la escritura de varios estándares, entre ellos (entre otras opciones de almacenamiento de datos) los estándares de Open Geospatial Consortium, Inc. (OGC) para entidades simples, el estándar de la Organización Internacional para la Estandarización (ISO) para tipos espaciales y los formatos espaciales de Oracle, PostGIS y Microsoft.
- Esri Grid: Es un formato de almacenamiento de datos raster nativo de ESRI. Hay dos tipos de grids: enteros y puntos flotantes. Utilizamos grids de tipo entero para representar datos discretos y grids de punto flotante para representar datos continuos. Los datos de elevación son un ejemplo de un grid de punto flotante.
- SVG (Scalable Vector Graphics): Es un formato gráfico basado en XML para crear archivos vectoriales en 2D, con un lenguaje de marcado por medio de etiquetas.
- XML (Extensible Markup Language): Es un lenguaje de etiquetas, es decir, cada paquete de información está delimitado por dos etiquetas como se hace también en el lenguaje HTML, permite jerarquizar y estructurar la información y describir los contenidos dentro del propio documento, así como la reutilización de partes del

mismo. La información estructurada presenta varios contenidos (texto, imágenes, audio, etc.) y formas: hojas de cálculo, tablas de datos, libretas de direcciones, parámetros de configuración, dibujos técnicos, etc.

- SGML (Standard Generalized Markup Language): Es un metalenguaje que cumple con el standard ISO 8879, permite definir distintos tipos de documentos y cuyos objetivos son: proceso de documentos por ordenador, separación de estructuras, contenido, y presentación e Independencia de sistemas y vendedores.
- Contingencias: Interrupción, no planificada, de la disponibilidad de recursos informáticos.
- Plan de Contingencia: Conjunto de medidas de detección y de reacción a poner en marcha ante la presencia de una contingencia.

IV.5.3 Lineamientos normativos.

IV.5.3.1 De los Objetivos de un Sistema de Video Vigilancia.

El Sistema de Video Vigilancia, como mínimo, debe ser implementado para atender las siguientes necesidades:

a) Dar seguimiento a vehículos en vialidades.
b) Vigilar cruceros.
c) Vigilar entradas y salidas a las ciudades.
d) Vigilancia de concentraciones públicas comerciales y recreativas.
e) La vigilancia de sitios de potencialidad delictiva.
f) Asistencia en eventos probables de protección civil.
g) Soporte a la administración municipal.
h) La vigilancia de entradas y salidas de zonas delictivas.
i) Vigilar y proteger instituciones de educación de nivel medio y superior.
j) Vigilar zonas de concurrencia turística y pasos fronterizos.
k) La integración de sistemas privados de video vigilancia externa.
l) Vigilar y proteger población infantil en Instituciones educativas básicas.
m) Protección de actividad económica productiva.
n) Cuidar el patrimonio público.
o) Respuesta pública efectiva.

IV.5.3.2 Sobre la atención de llamadas de emergencia.

Se debe usar la ecuación de Erlang o alguna similar para la estimación del número de operadores en el Sistema. Se puede usar alguna aplicación u hoja en Excel específica para estos cálculos.

IV.5.3.3 De la clasificación de los videos almacenados.

Los videos almacenados, como mínimo, deben estar separados lógica y físicamente tomando como referencias base a las siguientes categorías:

a) Videos del Flujo Diario.
b) Videos de Incidentes.
c) Videos de Evidencia.
d) Videos de Reserva en Sitio.

IV.5.3.4 Del almacenamiento de reportes.

a) Los reportes originados, como mínimo, deben ser almacenados en un gestor de base de datos que soporte el cifrado AES de al menos 128 bits en la longitud de llaves.
b) Cada reporte, como mínimo, debe tener un identificador único proporcionado automáticamente por el mismo gestor de la base de datos.
c) La Base de datos usada como repositorio de almacenamiento, como mínimo, debe ser de tipo Relacional. Si es de otro tipo, debe soportar el esquema relacional.
d) La Base de datos usada como repositorio de almacenamiento, como mínimo, debe soportar el lenguaje SQL Estándar en base a la norma ISO/IEC 9075-14:2011.

IV.5.3.5 Del almacenamiento de reportes de audio.

a) Cada audio debe estar vinculado con el reporte correspondiente usando el identificador único asociado al mismo.

b) Los archivos de audio, como mínimo, deben estar almacenados en un gestor de base de datos que soporte el cifrado AES de al menos 128 bits en la longitud de las llaves.
c) La Base de datos usada como repositorio de almacenamiento debe ser al menos de tipo Relacional. Si es de otro tipo, debe soportar también el esquema Relacional.
d) La Base de datos usada como repositorio de almacenamiento, como mínimo, debe soportar el lenguaje SQL Estándar en base a la norma ISO/IEC 9075-14:2011.

IV.5.3.6 Del tiempo de almacenamiento.

a) Para los Reportes de incidentes Verídicos el periodo de almacenamiento debe ser permanente.
b) Para los Reportes de incidentes no verídicos deben existir una serie de políticas internas para su tratamiento o eliminación.

IV.5.3.7 De la configuración de almacenamiento.

De la configuración de redundancia.

En su carácter de Centro de Datos (Data Center) para un contexto de seguridad, las configuraciones de almacenamiento deben respetar el nivel TIER IV para una disponibilidad del 99.991% (o al menos TIER III para ofrecer un 99.982%) de disponibilidad.

De la organización de los servidores

Los servidores usados para el almacenamiento de la información del Sistema de Llamadas de Emergencia y del video deben ser independientes lógica y físicamente

De la capacidad de almacenamiento

- Los formatos usados para almacenar los audios deben ser al menos de alguno de los siguientes formatos: aac, ac3, mp3.

- El texto se debe almacenar en formato binario.
- Se deben estimar los recursos necesarios para almacenar al menos un mes de audios, textos y reportes.

IV.5.3.8 Sobre las alertas.

- Como parte de la operación se deben definir al menos tres niveles de alertas.
- Debe existir un procedimiento asociado a cada nivel de alerta.
- Todo el personal debe conocer información sobre la alerta.
- Deben existir brigadas con roles específicos.
- Cada alerta se debe registrar detalladamente.

IV.5.3.9 Sobre la solicitud de grabaciones.

- Debe existir un procedimiento para recibir solicitudes de grabaciones.
- Cada solicitud debe estar completamente identificada.
- Cada solicitud debe registrarse electrónicamente.
- Si se imprimen formatos, todos deben describir detalladamente sobre qué es la información que se está entregando, los formatos, duraciones, llaves de encriptación entregadas, validez de las llaves de encriptación, y cualquier otra información que el SVV considere necesaria.

IV.5.3.10 De los reportes de incidentes.

- Debe existir un procedimiento para recibir solicitudes de grabaciones.
- Los reportes de incidentes deben registrarse en un sistema informático.
- Los reportes deben contener todo el detalle del incidente, y deben describir qué archivos almacenados dentro del SVV están asociados al mismo.

IV.5.3.11 De la Infraestructura Tecnológica.

Del corta-fuegos (Firewall).

Deben existir al menos dos cortafuegos instalados en el Centro de Datos. Se recomienda que se usen dos marcas diferentes con las mismas características técnicas.

La instalación del contrafuegos debe ser en base al nivel de redundancia TIER IV (o al menos TIER III) dependiendo del valor de disponibilidad buscado.

a) Debe al menos manejar los servicios de redes privadas virtuales.
b) Debe al menos manejar los protocolos de internet UDP, TCP, FTP, TFTP, DiffServe.
c) Debe al menos manejar los protocolos IPv4 e IPv6.
d) Debe al menos soportar a las Aplicaciones de Unicast y Multicast IP.
e) Debe al menos manejar de Calidad de Servicios QoS.
f) Debe al menos contener Puertos GbE.
g) Debe al menos soportar por lo menos 300 VLAN´s
h) Fuente de poder de respaldo debe soportar al menos una conmutación automática
i) Interfaz física y lógica deben al menos poder ser administradas en forma local por consola y/o remota a través del sistema de administración y gestión.
j) El equipo debe incluir los elementos necesarios de software y hardware, así como las licencias necesarias para su operación, gestión y administración correspondientes
k) El equipo debe contar con la versión liberada del sistema operativo más reciente y estable que tenga el fabricante
l) El Protocolo de administración y monitoreo debe al menos soportar SNMP V3, RADIUS
m) Los puertos o interfaces deben cumplir al menos con los siguientes estándares:
    a. IEEE 802.3,u,1p, ae, ab –ETHERNET (10/100/1000BASE-T)
    b. IEEE 802.1D – RSTP y MSTP
    c. IEEE 802.1Q – VLAN
    d. IEEE 802.1ag - CONNECTIVITY FAULT MANAGEMENT (CFM)
n) Debe tener al menos una fuente de poder redundante
o) Debe soportar al menos el estándar de EMC FCC 47 CFR Part 15 Class A
p) Debe respetar al menos la Norma UL60950-1

q) Debe ser de tipo Montaje en Rack 19”
r) Debe contar con una alimentación de 120 Volt AC
s) Temperatura de operación debe estar al menos entre 0 a 40 °C

De las pantallas de los Operadores de Video-Vigilancia.

- Las pantallas deben ser al menos de Tecnología LED al menos, aunque no se descartan las tecnologías emergentes.
- Las pantallas deben tener una resolución de al menos 1080p (1920x1080 pixeles).
- Las pantallas deben tener una relación de aspecto de al menos 16:9.
- El tamaño de la pantallas debe estar entre 26” y 32”. Si son de mayor tamaño deben ser evaluadas conforme a los estándares de ergonomía.
- Cada operador debe tener dos pantallas en su módulo de monitoreo. Si son más, deben ser evaluadas conforme a los estándares de ergonomía.
- Se deben tomar en cuenta las Normas ISO 11064-1, que contempla el diseño ergonómico de centros de control en forma de una metodología Top-Down, y las normas ISO-9241 y EN-ISO 9241, que establecen criterios de selección para equipos de visualización y de dispositivos de entrada.

De los servidores de almacenamiento para audio y reportes.

La instalación de los servidores deben estar de acuerdo al nivel TIER IV (o al menos TIER III) sobre disponibilidad y redundancia.

La interfaz de Red del servidor debe implementar una conexión de al menos 10Gb/s.

Los servidores deben soportar al menos discos duros SAS. Si las Unidades son de Estado Sólido (SSD) , además debe soportar los discos de tipo SAS. Si son de alguna tecnología emergente, todos los discos deben ser homologados.

El servidor, o los servidores que alojen la información deben de soportar arreglos RAID; como mínimo, configuración RAID 5. Y dentro del SVV, estar incluidos como parte del Centro de Datos con una configuración TIER IV (o al menos TIER III).

El Sistema Operativo instalado debe ser de tipo Servidor.

La cantidad de memoria RAM instalada debe basarse en las recomendaciones del manejador de bases de datos seleccionado.

Se deben elegir arquitecturas de al menos 64bits, tomando como referencia las recomendaciones del manejador de la base de datos.

Si se optó por usar un esquema de virtualización, el servidor que aloje tal virtualización debe cumplir con los siguientes recursos:

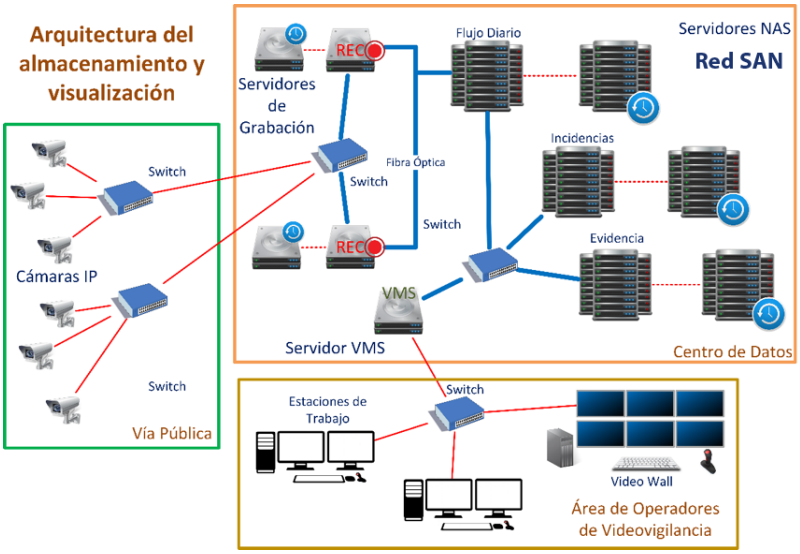
- Deben tomarse en cuenta los requerimientos recomendados por el sistema operativo que aloje la virtualización.
- Deben tomarse en cuenta los requerimientos recomendados por el software de virtualización.
- Se deben considerar los recursos a asignar para el sistema operativo que alojará al manejador de bases de datos.
- La Interfaz de red preferentemente debe ser de fibra óptica.
- El almacenamiento debe ser mediante discos duros SAS, siendo admisible el uso de Unidades de Estado Sólido (SSD) con soporte para discos SAS. Si son de otra tecnología emergente, se debe justificar técnicamente su compatibilidad con la infraestructura restante
- Debe incluir al menos dos Procesadores de última generación de preferencia Intel multi-núcleo de al menos 3.0 GHz de velocidad.
- Debe contar al menos con 64 GB en RAM.
- Debe soportar al menos arreglos de discos RAID 5.
- Debe tener al menos dos adaptadores de red independientes de acuerdo al esquema de redundancia propuesto por la recomendación TIER IV (o al menos TIER III).
- Debe tener al menos un adaptador de bus de host HBA de canal de fibra de 16 Gb de puerto doble.
- Debe tener al menos una fuente de alimentación redundante.

De los servidores de almacenamiento de video.

Los servidores de almacenamiento utilizados para el almacenamiento de video, deben ajustarse a las características de disponibilidad y redundancia establecidas por el nivel TIER IV (o al menos TIER III) establecidos en la Sección 3.6.1. Además, deben de contar con las siguientes características.

- Soporte e implementación del protocolo NAS para el almacenamiento en RED.
- Se debe de crear una SAN (Red de Área de Almacenamiento). Una SAN es una arquitectura completa que incluye una red de alta velocidad mediante fibra óptica entre los dispositivos que pertenecen a esta red. En la Figura IV.5.1, el área marcada como Red SAN forma la red área de almacenamiento.
- La interfaz de Red del servidor debe implementar una conexión de al menos 10Gb/s, esto puede ser mediante alguna de las interfaces disponibles en el mercado, se recomienda el uso de fibra óptica por sus bajos índices de latencia.
- Debe soportar discos duros SAS, esto no afecta el soporte de otras tecnologías, a menos que se determine el uso de Unidades de Estado Sólido (SSD), en cuyo caso se deben soportar adicionalmente los discos de tipo SAS
- Se recomienda contar con sistemas RAID basados en hardware para mejor rendimiento. En caso de optar por soluciones en software, el Sistema Operativo seleccionado debe de dar soporte a arreglos RAID; como mínimo, configuración RAID 5.Los sistemas operativos que dan soporte son los clasificados como Sistemas Operativos de Servidor, tales como Windows Server NT y superiores, y aquellos basados en Unix.

Figura IV.5.1 Arquitectura del almacenamiento y visualización



De la arquitectura para servidores de almacenamiento.

La instalación de los servidores debe estar de acuerdo al nivel TIER IV (o al menos TIER III) de disponibilidad y redundancia.

Deben cumplir con el estándar TIER IV (o al menos TIER III) definido por el estándar ANSI/TIA-942-A para Centro de Datos Tolerante a fallas.

Debe existir una separación física entre los servidores de grabación y almacenamiento
Debe existir una separación de los diferentes tipos de videos: al menos de flujo diario, de incidencias y de evidencia.

De las características para las estaciones de trabajo.

La determinación de las características finales de los equipos deben tomar en cuenta las normas ISO-9241 y EN-ISO 9241.

La estación de trabajo y sus componentes básicos que se utilizan en las salas de videovigilancia y atención de llamadas de emergencia, deben cumplir al menos con los siguientes requerimientos:

- El Procesador debe ser de última generación para estaciones de trabajo disponible en la fecha de adquisición. Preferentemente Intel multi-núcleo con una velocidad de al menos 3.0 GHz
- La memoria instalada debe ser de al menos 8 GB, Memoria DDR4 de al menos 2133MHz de velocidad, con paridad [ECC] (4 RDIMMs)
- El disco duro debe tener una capacidad mínima de 1TB de tecnología SAS, o SSD u otra tecnología emergente justificando técnicamente su compatibilidad con lo instalado
- La Tarjeta de video debe tener al menos 2 GB de memoria de gráficos, 128 bits de amplitud de interfaz de memoria, 160 Gbps de ancho de banda de memoria y soporte para pantalla VGA, HDMI, Display Port.

Del mouse.

El mouse que se debe usar por los operadores de videovigilancia y de atención de emergencias debe tener al menos las siguientes características:

- Debe ser conectado a través de USB.
- Debe usar una tecnología de Detección de Movimiento Óptico.
- Debe permitir ser configurado para tener una orientación para diestro o zurdo
- Del teclado.
- El teclado que se debe usar por los operadores de videovigilancia y de atención de emergencias debe tener al menos las siguientes características:
    - Debe ser conectado a través de USB.
    - Debe ser con una distribución de teclas tipo QWERTY y en español.

Del joystick o palanca de control para cámaras PTZ.

El joystick que se debe usar por los operadores de videovigilancia debe tener al menos las siguientes características:

- El Joystick debe ser con efecto de Hall de tres ejes: X/Y: para movimiento vertical y horizontal, Z: botón para el zoom.
- Debe tener al menos 6 teclas de acceso directo a aplicaciones definidas.

Del UPS para equipos de monitoristas.

El UPS que se debe usar por los equipos de los operadores de videovigilancia y de atención de emergencias debe tener al menos las siguientes características:

- Debe contar con un Supresor de picos y ruido integrado.
- Debe tener Corrección de voltaje integrado.
- Debe tener un Sistema de LED's para verificar estado del equipo.
- Debe permitir una Carga en modo off y función de arranque en frío.Debe ser de Tecnología Trifásico doble conversión online.
- Debe ser de al menos una Potencia de 20 KVA.
- Debe soportar un Voltaje de entrada de 208/120V o 220V/127V.
- Debe soportar un Voltaje de salida de 220V/127V.
- Debe trabajar con una Frecuencia de 50/60 Hz con detección automática.
- Debe tener un regulador de voltaje.
- Debe soportar un respaldo mínimo de 15 minutos.

Del software de monitoreo de redes.

El objetivo del software es permitir detectar, diagnosticar y resolver problemas de rendimiento de redes e interrupciones con rapidez.

Debe tener al menos las siguientes características:

- Debe poder responder a múltiples verificaciones de condiciones, eventos correlacionados, topología de red, y dependencias del dispositivo.
- Debe acelerar la detección y solución de problemas, mejorarlos niveles de servicio y reducir el tiempo de inactividad de la red.
- Debe permitir monitorear y generar informes de dispositivos de red de varios proveedores compatibles.
- Debe ser escalable sin restricciones tecnológicas que lo hagan obsoleto.
- Debe permitir monitorear el rendimiento y la disponibilidad de las interfaces y dispositivos de red y los indicadores de rendimiento, como uso del ancho de banda, pérdida de paquetes, latencia, errores, y descartes.

- Debe permitir inspeccionar y analizar exhaustivamente paquetes.
- Debe permitir identificar rápidamente reducciones y cambios en el rendimiento de las aplicaciones y capacidad de determinar si ha sido la aplicación o la red la que ha causado el cambio.
- Debe ser independiente de los sistema operativo.
- Debe permitir el monitoreo remoto mediante túneles SSL cifrados o SSH.
- Debe permitir programar Plugins específicos para incorporar nuevos sistemas o características.

Del sistema de comunicación en los módulos de monitoreo.

Del teléfono.

El teléfono que se debe usar en las salas de atención de llamadas de emergencia y en los módulos de video-vigilancia, así como su auricular, deben cumplir al menos con los siguientes requerimientos:

- El teléfono debe tener altavoz.
- El teléfono debe tener identificación de llamadas.
- El teléfono debe contar con al menos las siguientes Teclas de funciones fijas: correo de voz, ID de llamada, llamada en espera, transferencia de llamada, conferencia tripartita.
- El teléfono debe incluir una Pantalla de cristal líquido monocromático con revestimiento anti-reflejante de al menos 2 líneas X 24 caracteres.
- El teléfono debe incluir un Soporte para auriculares alámbricos.

De la diadema o auricular.

La diadema o auricular debe cumplir al menos con las siguientes características:

- Debe contar con un Micrófono con ultra-anulación de ruido (UNC).

- Debe contar con un Micrófono largo para proporcionar mejor control de ecos y anulación de ruidos del sector.
- Debe incluir un brazo de micrófono flexible con posiciones, que se mantenga en su posición para una transmisión de voz nítida.
- Debe ser con audio de banda ancha de la mayor calidad que cumpla con los estándares TIA920A.
- Debe ser compatible con el teléfono a utilizar.

De los radios para comunicación interna.

Radios de seguridad (Terminal digital portátil).

Los radios de seguridad deberán tener por lo menos las siguientes especificaciones técnicas generales para que puedan integrarse a la Red Nacional de Telecomunicaciones:

- Terminal digital portátil (radio)
    - Debe trabajar en un Rango de frecuencia: 380 - 430 MHz con espaciado de canales de 10 a 12.5 KHz.
    - Debe tener una Potencia máxima de salida del transmisor: 2W.
    - Debe tener una Sensibilidad estática / dinámica mejor que -119 dBm / -111dBm.
    - Debe contar con una Pantalla TFT activa en color de alta resolución de 130 x 130 píxeles
    - Debe tener una Autonomía de al menos 12 horas
    - Debe tener un Tiempo de carga máximo de 2,5 horas
    - Debe ser Resistente al polvo y agua conforme a la especificación IP54.
    - Debe ser Resistente a golpes, caídas (2 metros) y vibraciones según la especificación ETS EN 300019-1-7 clase 5M2.
    - Debe contar con al menos una Conexión a PC a través de controladores TETRAPOL.

- Debe tener al menos un Cifrado incluido extremo a extremo para voz y datos.
- Debe permitir al menos enviar Mensajes de texto e intercambio de datos TETRAPOL
- Debe tener un Teclado alfanumérico
- Debe tener al menos Teclas de volumen, PTT, botón rojo para llamadas de emergencia.
- Debe contar con un Botón rotativo para ajuste de volumen y/o selección de canal.
- Debe tener un Identificador de llamada entrante.
- Debe tener tecnología Bluetooth integrada.

- Terminal digital móvil (radio). Debe tener al menos las siguientes características:
  - Debe tener una Potencia de salida del transmisor: hasta 10 W.
  - Debe tener una Sensibilidad estática / dinámica mejor que -119 dBm / -111dBm.
  - Debe trabajar al menos en las Bandas de frecuencia: 380-430 MHz con espaciado de canales de 10 a 12.5 kHz y 440-490 MHz con espaciado de canales de 10 a 12.5 kHz
  - Debe permitir un Posible desplazamiento de medio canal.
  - Debe tener una Antena GPS integrada.
  - Debe ser Resistente al polvo y agua conforme a la especificación IP54.
  - Debe ser Resistente a golpes, caídas (2 metros) y vibraciones según la especificación ETS EN 300019-1-7 clase 5M2.
  - Debe trabajar en un Rango de temperatura de trabajo de -30 °C a 60 °C.
  - Debe incluir una Pantalla gráfica TFT de al menos u tamaño de 2.2", de alta resolución con al menos 128 x 160 pixeles.
  - Debe integrar un esquema de Manos libres
  - Debe tener un Teclado alfanumérico
  - Debe permitir al menos un Intercambio de datos de tipo TETRAPOL
  - Debe integrar al menos un Cifrado extremo a extremo para voz y datos
  - Debe permitir realizar Llamadas individuales y de grupo.
  - Debe permitir Llamadas PBX / PSTN

- Debe permitir Transferencia de llamadas
- Debe permitir Llamadas de emergencia.
- Debe incluir Identificador de llamadas.

De las características de la Radio Base.

- Debe tener una Terminal digital de escritorio (radio base), con al menos las siguientes características:
    - Debe tener una Potencia de salida del transmisor: hasta 10 W.
    - Debe tener una Sensibilidad estática / dinámica mejor que -119 dBm / -111dBm.
    - Debe poder trabajar en las Bandas de frecuencia: 380-430 MHz con espaciado de canales de 10 a 12.5 kHz y 440-490 MHz con espaciado de canales de 10 a 12.5 kHz.
    - Debe incluir Antenas de la estación base.
    - Debe tener Fuentes de alimentación redundantes.
    - Debe incluir al menos un Puerto Ethernet.
    - Debe dar Cumplimiento a las normas ETSI / TETRA.
    - Debe incluir al menos una Interfaz RDSI para conectar a PSTN.
    - Debe incluir un Cifrado extremo a extremo para voz y datos.
    - Debe permitir una Gestión de llamadas y despacho.
    - Debe permitir un Intercambio de datos TETRAPOL.
    - Debe incluir un Cifrado extremo a extremo para voz y datos.
    - Debe permitir Llamadas individuales y de grupo.
    - Debe permitir Llamadas PBX / PSTN.
    - Debe permitir Transferencia de llamadas.
    - Debe permitir Llamadas de emergencia.
    - Debe incluir un Identificador de llamadas.
- Debe incluir Baterías para terminal digital portátil.
- Debe tener una Batería interna BLN-Ex, Li-Poly de 1400 mAh o alguna compatible con la terminal digital portátil.
- Debe incluir un Cargador múltiple o individual para terminal digital portátil
    - Cargador de mesa DCR-1.
    - Cargador para viajes ACP-12E (CE).
- Debe incluir un Cargador de automóvil LCH-12 (sólo en caso de ser requerido).

De las paredes de video (Videowalls).

- Se debe realizar un estudio y justificar la necesidad de instalar una pared de video. Si es así, debe ser independiente a la zona de monitoreo en un área denominada sala de crisis.
- Se debe realizar un estudio para determinar el tamaño de la pantalla, forma y resolución, según la tecnología seleccionada para obtener el mayor beneficio
- Se debe realizar un estudio para obtener los mejores valores de ajustes de imagen (brillo, color, controles y sistemas de iluminación).
- Se debe realizar un estudio para obtener el máximo desempeño en base a los factores de entorno (luz ambiental, ruido, colores del entorno).
- Se debe analizar su impacto en el presupuesto.
- Se debe analizar la relación costo beneficio que incluya como parámetros la densidad de pixeles y el número de pantallas.

IV.5.3.12 De la gestión de video.

Del sistema de gestión de video.

- Debe tener un Control de Acceso Unificado para el manejo de videos.
- Debe ser un Sistema federado que permita el escalamiento y la monitorización de sitios independientes remotos como si fueran parte de un solo sistema virtual.
- Debe permitir una Administración de los niveles de amenazas que permita cambiar la configuración del sistema de seguridad de manera instantánea, en respuesta a las condiciones cambiantes en seguridad y de amenazas potenciales en base a ajustes definidos previamente.
- Debe permitir una Gestión de alarmas que permita configurar las alarmas y los flujos de trabajos en base a multitud de eventos del sistema, tales como la detección de movimiento y alarmas de puertas, y asigne responsabilidades a sus operadores.
- Debe incluir un Sistema de reconocimiento de placas (LPR).

- Debe contar con una única Interfaz de gestión centralizada que ofrezca una eficiente administración del sistema de todas las cámaras y dispositivos conectados, independientemente del tamaño del sistema y la distribución.
- Debe permitir el Bloqueo de evidencias para garantizar la disponibilidad de las grabaciones para investigaciones y que permite ampliar manualmente el tiempo de retención omitiendo las políticas normales de archivado y de limpieza de vídeo.
- Debe incluir mecanismos de Cifrado de base de datos de vídeo y firma digital usando el estándar AES con llaves de al menos 128 bits.
- Debe permitir la Transmisión múltiple en directo que permita varias transmisiones para visualización en directo con distintas propiedades en función del ancho de banda disponible.
- Debe contar con una Conexión hacia los sistemas de despacho asistidos por computadora (CAD) y de ubicación geográfica con las respectivas capas de cámaras (GIS).
- Debe tener Interacción con los sistemas de geo localización de unidades (AVL).

De la clasificación de video.

- Los videos deben estar codificados usando el estándar H.265 con soporte para H.264.
- Debe tener una resolución mínima de 720x1280 píxeles, pero la deseable es de 1080p.
- Debe tener una frecuencia mínima de refresco de 30 cuadros por segundo.
- Los videos recibidos se deben catalogar de forma separada de acuerdo a las siguientes clases: flujo diario, incidentes, evidencia, reserva en sitio.

De los formatos de video.

- Las grabaciones de video deberán usar un formato de compresión de H.265, con soporte para H.264.

- Debe tener una resolución mínima de 720x1280 píxeles, pero la deseable es de 1080p.
- Para cámara de 1.3 MP o superiores, se debe usar una configuración de al menos 30 fps.

De los sistemas de respaldo.

- El Centro de Datos debe ser tolerante a fallas en base al estándar ANSI/TIA-942-A y se nivel TIER IV (o al menos TIER III) para ofrecer una disponibilidad de al menos 99.991%, deseable de 99.995%.
- La configuración de los discos debe ser de al menos tipo RAID 5.
- Debe haber instalado un servidor espejo de almacenamiento para cada tipo de video que se almacena.
- Los discos de almacenamiento deben ser de tipo SAS. Es posible tipos SSD o alguna tecnología emergente siempre y cuando se justifique su compatibilidad con los tipos ya instalados.
- Si los discos de almacenamiento son de tipo SSD u otra tecnología emergente, se debe soportar de manera adicional el tipo SAS.
- No se debe mezclar en una misma arquitectura (servidor) discos SAS, con SSD u otra tecnología diferente.

De la disponibilidad de video.

- Los datos correspondientes a los videos almacenados deben estar disponibles para las áreas de los Centros de Control y Comando a través de la intranet.
- Los equipos de almacenamiento estarán ubicados en un espacio dedicado exclusivamente para este fin, tales espacios se considerarán Centros de Datos que deben cumplir el TIER IV (o al menos TIER III) definido por el estándar ANSI/TIA-942-A.

- Cada grabación almacenada en el Centro de Datos será protegida para su acceso según sea su tipo. Los mecanismos y las clasificaciones las determina el Centro de Control.

Del Plan de Almacenamiento de video.

- Las grabaciones clasificadas como flujo diario deben permanecer almacenadas durante un mínimo de 15 días naturales. Se recomienda almacenar durante 30 días naturales.
- Las grabaciones clasificadas como incidente deben permanecer almacenadas durante un mínimo de seis meses.
- Las grabaciones clasificadas como evidencia deben permanecer almacenadas durante un mínimo de dos años o durante el periodo que sea necesario si una autoridad jurisdiccional lo solicita o es justificado por el C4.
- Las grabaciones clasificadas como reserva en sitio deben permanecer almacenadas por un tiempo mínimo de 24 horas.
- Se debe poder almacenar el video de todas las cámaras instaladas, más un 25% de espacio recomendado por los estándares.
- Todos los videos deben ser almacenados usando el estándar AES con al menos llaves de 128 bits. Las llaves de encriptación deben ser establecidas preferentemente por el personal que administre el SVV.

Del uso de mapas interactivos.

- El SVV debe incluir como parte de su infraestructura de software, a un Sistema de Georreferenciación que incluya la ubicación de las cámaras e integre la información sobre incidentes y estadísticas generadas por el Departamento de Inteligencia y Análisis.
- El Sistema de Georreferencias debe soportar los estándares para representación de mapas. De manera mínima debe poder incorporar los formatos Shapefiles

(SHP), Keyhole Markup Language (KMZ/KML), GDB (File Geodatabase), ArcInfo, ArcSDE, Esri Grid, SVG, XML, SGML.

- Debe permitir el acceso a mapas temáticos para el apoyo a las tareas de monitorización, seguimiento y toma de decisiones.
- Debe permitir la Creación de capas en el mapa.
- Debe permitir la Localización y la ubicación interactiva de cámaras.
- Debe permitir la Selección de cámaras directamente desde el mapa para su visualización.
- Debe permitir Mostrar notificaciones de alarmas y de eventos.

IV.5.3.13 Sistema de Video Vigilancia Interno.

- El centro debe contar con un circuito cerrado de televisión (CCTV) interno, éste tiene como finalidad, fortalecer las medidas de seguridad en las zonas internas y perimetrales del centro, reforzar la seguridad del personal y el resguardo de los bienes muebles e inmuebles, documentales e informáticos.

- Las características tecnológicas deben ser las mismas usadas para el SVV descrito en cuanto a pantallas, mesas de trabajo, equipo de apoyo, y cualquier elemento necesario para llevar a cabo esta actividad.

De la interoperabilidad con sistemas de Video Vigilancia privados.

- Por razones de seguridad el centro podrá generar acuerdos para tener acceso a Sistemas de Video Vigilancia privados que sean compatibles tecnológicamente con el estándar.
- El centro podrá monitorear la información de estos sistemas preservando protocolos de seguridad y operativos que cumplan con el estándar.

- Idealmente se deberá contar con un software que garantice el acceso y esté integrado al CAD, permitiendo contar con un registro de seguimiento y el almacenamiento de la información del evento en un solo folio.
- La información almacenada podrá ser compartida a las instancias de procuración de justicia que así lo soliciten, de manera oportuna y mediante protocolo que se establezca con el centro.

Del Cuarto de Control.

- La Coordinación General debe establecer un Cuarto de Control con la finalidad de coordinar el flujo de comunicaciones que permitan una rápida y eficiente respuesta ante el impacto de agentes perturbadores traducidos en riesgos y daños a los trabajadores; así como, bienes muebles e inmuebles del centro.

- El Cuarto de Control debe permitir al menos administrar, manejar, adecuar, actualizar y mantener los sistemas de Radiocomunicaciones, Circuitos Cerrados de Televisión, Monitoreo de las Centrales de Alarmas y Vigilancia Periférica.

- El Cuarto de Control debe ser ubicado en las instalaciones del centro, manteniéndose en operación permanente mediante la red interna con atención las 24 horas del día.

De los sistemas de respaldo de energía.

- La acometida o acometidas principales de la CFE al edificio donde se encuentra localizado el SVV debe ser subterránea, con la profundidad establecida por la misma CFE para instalaciones de prioridad.
- Debe haber una doble trayectoria de alimentación para los equipos de cómputo.

Características básicas de cada UPS asignado por módulo de trabajo o servidor.

- Debe contar con un Supresor de picos y ruido integrado.
- Debe tener Corrección de voltaje integrado.
- Debe contar con un Sistema de LED’s para verificar estado del equipo.
- Debe permitir una Carga en modo off y función de arranque en frío.

Características básicas de cada Sistema de Energía Ininterrumpida.

- Debe tener una Alimentación basada en Diesel.
- Debe contar con un Supresor de picos y ruido integrado.
- Debe tener Corrección de voltaje integrado.
- Debe contar con un Sistema de LED's para verificar estado del equipo.
- Debe tener un Sistema de arranque automático.
- Debe estar resguardada siguiendo las mismas políticas que el equipo de cómputo que está en el interior del CC del SVV.

Del mantenimiento.

- La instalación y mantenimiento de las cámaras del sistema de video vigilancia deberá ser efectuado por empresas debidamente habilitadas y registradas por la autoridad competente.
- Todas las cartas garantía de los equipos deben ser entregadas a la Entidad contratante. La garantía post-instalación debe ser de al menos tres meses. Posterior a este periodo obligatorio para la empresa, se pueden contratar servicios de mantenimiento adicionales.
- Las características de estos servicios de mantenimiento adicional son:
    - Deben ser ofrecidos en términos de 24/7.
    - En base a que el servicio de video vigilancia debe ser prestado en un porcentaje del 99.995%, los tiempos de respuesta de todo el equipo involucrado con la afectación de este porcentaje debe recibir el mantenimiento correspondiente. La empresa, en base a su experiencia instalando este tipo de equipos debe considerar tener en Stock, el equipo suficiente para poder otorgar el servicio antes mencionado.
    - Se recomienda que personal de la Dirección de Tecnologías de Información y Telecomunicaciones sea capacitado por la misma empresa en un proceso de transferencia tecnológica, para que la dependencia con la Empresa que realizó la instalación sea mínima.

Del mantenimiento correctivo.

- La primera opción en mantenimiento correctivo debe ser por reemplazo.
- Cada falla debe ser documentada por el sistema almacenando al menos: Identificación de la necesidad, Programación de visita técnica y Ejecución del servicio.
- El personal del centro debe corroborar la identidad del personal de servicio técnico, solicitando la presentación del gafete respectivo y se debe efectuar la confirmación del nombre y documento de identidad del mismo con el servicio técnico.
- El personal del centro debe facilitar el acceso del personal de servicio técnico a las áreas donde se encuentran instalados los equipos objeto de la revisión, una vez finalizada la visita, el personal de servicio técnico contratado debe entregar un reporte técnico donde se indique: El diagnóstico relacionado con la falla detectada y la descripción abreviada del procedimiento que se empleó para su detección, así como las acciones correctivas implementadas. Este reporte técnico debe ser firmado por el director de tecnologías.
- En caso que no sea posible suministrar una solución durante la visita y se deba realizar visitas posteriores con el fin de realizar un procedimiento de seguimiento para la detección de la causa de la falla, el servicio técnico debe informar a quien firma el reporte acerca de las pruebas a realizar y su duración. La hora de salida en el reporte técnico debe ser diligenciada por el personal del centro que firma el reporte.

Del mantenimiento preventivo.

Para establecer los planes de mantenimiento deben considerarse en primera instancia los manuales de usuario de los equipos, en los cuales se establecen los periodos de mantenimiento de este tipo para cada uno de los equipos. Deben planearse todos los

mantenimientos que se realizarán, las fechas, las mecánicas, los formatos y las evidencias al momento de firmar los contratos para este fin.

Seguridad Interna.

- Los sistemas de acceso interno para las zonas de operación y las zonas de servidores y respaldo de video y audio deben ser redundantes, esto es, usar dos mecanismos de identificación. Se deben evitar los accesos solo con la llave de puertas.
- Todas las identificaciones del personal interno deben actualizarse por lo menos dos veces al año.
- Las identificaciones de los visitantes temporales deben ser entregadas al entrar y retiradas al salir del C4.
- Debe ser establecido un mapa de seguridad dentro del C4, y establecer los tipos de accesos permitidos en cada área del mapa. Las credenciales de acceso deben ser validadas conforme al mapa y emitir alertas en caso de intentos de violación.
- El acceso de todo visitante debe ser aprobado por un empleado autorizado.
- Los gafetes para visitantes se proporcionarán al entregar una identificación oficial.
- Los gafetes deben regresarse cuando el visitante abandona el centro control.
- Los visitantes siempre deben estar acompañados dentro del centro de control y portar el gafete a la vista en todo momento.
- El acceso a los visitantes solo debe permitir entrar al área o áreas establecidas desde que se entrega el gafete.
- El gafete debe tener un número de serie y debe de tener un diseño (por ejemplo: color o forma) distinto al de los empleados.
- Se debe llevar un registro de cada uno de los visitantes, deberá contener el nombre completo, fecha, persona que se visitó, área o áreas que visitó y motivo de la visita.

Seguridad Perimetral.

- El sistema de seguridad, desde el punto de vista balístico, debe ser de nivel 3, esto es, que los muros exteriores del centro soporten disparos de armas calibre 45 o la explosión de una granada.
- Debe contar con un vigilante externo o cámara que detecte algún tipo de movimiento que pueda poner en riesgo las instalaciones del centro de control.
- Debe tener en la puerta un relé de alta seguridad para controlar la apertura y cierre de las puertas, y debe controlarse mediante un operador remoto (a través de la red) o ser una respuesta automática a un evento de alerta. Si existen credenciales electrónicas de empleados, el sistema debe usar validación redundante (credencial y teclado para PIN de seguridad) para abrir los accesos de manera remota.

Sistema Contra Incendios.

- Debe existir un sistema contra incendios con agentes limpios (gases limpios). La periferia del centro de control debe estar protegida contra incendios, ya sea con agua o con cualquier otro agente. Las paredes, pisos, techos y puertas deben soportar un fuego que dure 90 minutos a 1,000 grados centígrados.
- Las medidas tomadas deben ser de acuerdo con la Norma Oficial Mexicana NOM-002-STPS-2010 [V.13], sobre las condiciones de seguridad, prevención y protección contra incendios en los centros de trabajo.
- El plan de atención a emergencias de incendio deberá contener, según aplique, lo siguiente:
    - La identificación y localización de las áreas y equipos que impliquen riesgo de incendio.
    - Se deben identificar las rutas de evacuación, salidas y escaleras de emergencia, zonas de menor riesgo y puntos de reunión, entre otros.
    - Se debe definir el procedimiento de aviso, en caso de ocurrir una emergencia de incendio, con base en el mecanismo de detección implantado.

- Se deben definir los procedimientos para la operación de los equipos, herramientas y sistemas fijos contra incendio, y de uso del equipo de protección personal para los integrantes de las brigadas contra incendio.
- Se debe definir el procedimiento para la evacuación de los trabajadores, contratistas, patrones y visitantes, entre otros, considerando a las personas con capacidades diferentes.
- Se debe definir el plan de ayuda mutua que se tenga con otros centros de trabajo;
- Se deben definir los procedimientos para el retorno a actividades normales de operación, para eliminar los riesgos después de la emergencia, así como para la identificación de los daños.
- Se debe establece la periodicidad de los simulacros de emergencias de incendio por realizar.
- Se deben definir los medios de difusión para todos los trabajadores sobre el contenido del plan de atención a emergencias de incendio y de la manera en que ellos participarán en su ejecución.

Plan de Contingencia Contra Desastres.

- El Centro de Control debe diseñar un Plan de Contingencias junto con las autoridades competentes estatales y federales, y considerando la prioridad de los sistemas que se están poniendo en riesgo.
- Cada CC debe contar con una serie de procesos documentados que establezcan las acciones a realizar ante un evento que ponga el riesgo de las instalaciones o al personal que labora en ellas.

IV.6 Operación

IV.6.1 Resumen

La Norma técnica para estandarizar las características técnicas y de interoperabilidad de los SVV para la seguridad pública tiene, entre otros, el objetivo de contar con herramientas técnicas y administrativas que coadyuven a garantizar la operación, funcionamiento y escalamiento de las Unidades de Video Vigilancia, bajo las directrices del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, para conseguir sus objetivos y metas propuestas en el Sistema Nacional de Seguridad Pública (SNSP). Este apartado contiene los criterios de definición de la operación, estructura, organización y funcionalidad de dichas Unidades, además de los puestos que implica su operación.

Los tres órdenes de gobierno han implementado modelos de organización y operación de los Centros de Control de SVV. Sin embargo, estos esquemas varían de acuerdo a la complejidad de los delitos o su gravedad, pero también por los recursos destinados a su combate. A pesar de que los recursos asignados a la operación son importantes, todavía prevalecen áreas de oportunidad en la operación.

La capacitación de los operadores del SVV es crucial para un funcionamiento óptimo del sistema. Los recursos humanos deben tener la capacidad de leer las situaciones que se despliegan en la pantalla y actuar en consecuencia. Un Centro de Control es un espacio que proporciona servicios de atención y despacho de emergencias de manera oportuna, mediante equipo y sistemas tecnológicos que permiten la oportuna toma de decisiones y la correcta ejecución de acciones para una pronta y eficaz respuesta a solicitudes de la población.

Durante las visitas realizadas a algunos Centros de Control en la elaboración de este documento, se encontraron procesos administrativos, esquemas de coordinación y procesos de calidad que representan buenas prácticas. Estas medidas han sido incorporadas a un modelo de organización robusto que persigue la calidad en el servicio y la eficiencia en la operación.

La estandarización de la operación es un punto central en la implementación de un SVV. Una entidad podría contar con tecnología de punta, instalaciones de primer nivel y, aun así, subutilizar sus recursos para el combate al crimen mediante SVV debido a una deficiente capacitación del personal, una excesiva burocracia o una falta de coordinación entre los niveles. Llegado este punto, la Norma busca establecer parámetros que garanticen que el componente humano está al nivel de preparación óptimo para un aprovechamiento integral del sistema.

IV.6.2 Glosario.

Para contextualizar la información en el ámbito de la presente Norma, se presenta a continuación un glosario de términos y definiciones relacionadas.

- Capacidades: conocimientos. habilidades, actitudes y valores expresados en comportamientos, requeridos para el desempeño de un puesto dentro del Sistema de Servicio Profesional de Carrera en la Administración Pública Federal Centralizada.
- Catálogo de Puestos: Es el instrumento que contiene los puestos, elaborados por la SFP o aquellos que las instituciones soliciten su inclusión en dicho instrumento, a fin de contar con información que pueda ser utilizada de manera transversal en la Administración Pública Federal.
- Catálogo Institucional de Puestos: El Catálogo Institucional de Puestos de la Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública.
- Certificación de capacidades: Proceso por el cual se determinan aptitudes mediante la confirmación del nivel de dominio de los conocimientos y habilidades de un servidor público, así como sus actitudes, mediante la evaluación de las conductas propias de cada capacidad. La certificación de capacidades tendrá efectos para fines de ingreso, de permanencia o de desarrollo profesional, según corresponda.
- Centro de control y comando: Es el área que proporciona servicios de seguridad pública, atención y despacho de emergencias de manera oportuna mediante equipo y sistemas tecnológicos que permiten la oportuna toma de decisiones y correcta ejecución de acciones para la pronta y eficaz respuesta a la población.

- Criterio o directriz: Es la política de acción elegida como guía en el proceso de toma de decisiones al poner en práctica o ejecutar las estrategias, programas y proyectos específicos de nivel institucional.
- C4: Centro de control, comando, cómputo y comunicación; es la unidad administrativa que coordina a las instituciones o instancias de seguridad pública de los tres órdenes de gobierno, encargada de la integración, administración, operación, vigilancia y desarrollo de los sistemas tecnológicos aplicados a la seguridad pública, así como los servicios de emergencia y de denuncia anónima que se prestan a la población.
- Comunicaciones: Apoyar las necesidades de comunicación para establecer o brindar servicios de videovigilancia, radiocomunicación, telefonía e internet en los Centros de Control y Comando. Se cuenta con herramientas como MPLS, Internet dedicado, GPRS, enlaces dedicados de radio (microondas) y/o fibra óptica.
- Cómputo: Mantener en óptimas condiciones los equipos de la red LAN del centro de control, así como los servicios de voz y el mantenimiento de las llamadas al centro de atención de emergencias. Solucionar los problemas de la red de videocámaras y los relacionados con la Seguridad Lógica de la Red, de la manera más rápida posible, de tal manera que los servicios que se tienen usando sobre dicha red, estén disponibles las 24 horas y de esta manera optimizar recursos y costos de operación. Mantener en óptimo funcionamiento la red de microondas para el transporte de datos, instaladas en las casetas de radiocomunicación, así como configurar los equipos de CCTV utilizados en la vigilancia interna de los subcentros y las casetas de comunicación Se cuenta con algunos equipos activos como servidores, workstation, sistemas de almacenamiento, computadoras.
- Coordinación: Diseñar la estructura organizativa para coordinar eficazmente los recursos tanto locales como federales, involucrados en la atención a emergencias, crisis y desastres mayores, para su reacción inmediata. Establecer la conexión de tareas del personal para que se lleven a cabo y así lograr los objetivos del Centro de Control y Comando.
- Descripción de puestos: Es el proceso que permite su ubicación, identificación y análisis en el contexto organizacional.
- Despacho: Proceso de canalización de la solicitud a las instalaciones y/o dependencias responsables en la atención directa de la emergencia y en el cual

pueden intervenir instancias oficiales o corporaciones de apoyo. Se realiza principalmente a través de los sistemas de radiocomunicación, vinculados a la video vigilancia para el monitoreo urbano.

- Equidad: Es la igualdad de oportunidades, sin discriminación por razones de edad, raza o etnia, condiciones de salud, capacidades diferentes, religión o credo, estado civil, condición social o preferencia política.
- Equidad de género: Es la igualdad de oportunidades para cualquier persona sin distinción de su sexo.
- Especialistas: Servidores públicos responsables de analizar y procesar la información que se genere por virtud de la descripción, elaboración de perfiles y valuación de puestos.
- Estructura ocupacional: Conjunto de puestos con actividades definidas, delimitadas y concretas que permiten el cumplimiento de una función con base en los registros y autorizaciones, en los términos de las disposiciones aplicables.
- Estructura orgánica: Unidades administrativas que integran las Unidades de Monitoreo, donde se establecen niveles jerárquico-funcionales de conformidad con la competencia que se les asigna en el Reglamento Interior del Secretariado Ejecutivo. De esta forma se identifica el sistema formal de la organización, a través de la división de funciones y la jerarquización de sus mandos, en la que se establece la interrelación y coordinación de los mismos.
- Estructura orgánica básica: Área que integran las unidades administrativas del Secretariado Ejecutivo cuyas funciones reflejan las atribuciones conferidas en la Ley General del Sistema Nacional de Seguridad Pública. Se caracterizan por tomar decisiones, formular políticas, elaborar directrices y determinar líneas generales, que se vinculan en forma directa y determinante con los objetivos institucionales. Comprende áreas con nivel jerárquico-organizacional de Secretario hasta Director General y sus equivalentes.
- Estructura orgánica no básica: la integran las unidades administrativas cuyo nivel jerárquico-organizacional es menor a Director General y depende invariablemente de alguna unidad ubicada en la estructura orgánica básica. Dichas unidades se caracterizan por diseñar, elaborar, realizar estudios y trabajos, así como aplicar las

políticas, programas y normas establecidas que coadyuven a alcanzar los objetivos institucionales determinados.

- Evaluación del desempeño: son los procesos, métodos y mecanismos de medición cualitativos y cuantitativos, del cumplimiento de las funciones y metas individuales y colectivas de los servidores públicos de carrera, en función de las capacidades y del perfil determinado para el puesto que ocupan.
- Función Sustantiva: Puestos con impacto directo en la razón de ser de la institución. Están orientados hacia las áreas funcionales no administrativas de la institución.
- Función administrativa / adjetiva: Puestos con impacto indirecto orientado a la administración de la institución, cuya función es relevante para el desarrollo de la gestión interna de la institución. De conformidad con el Art. 20 de la LOAPF tienen como función brindar servicios de apoyo administrativo en materia de planeación, programación, presupuesto, informática y estadística, recursos humanos, recursos materiales, contabilidad, fiscalización, archivos.
- Inteligencia: Aportar información estratégica para la ejecución de acciones, la elaboración de estrategias y el diseño de políticas públicas que permitan disuadir, contener y neutralizar riesgos y amenazas a la seguridad.
- LSPCAPF: ley del Servicio Profesional de Carrera en la Administración Pública Federal.
- Nombramientos temporales: son aquellos que se pueden efectuar para ocupar un puesto, una vacante o una plaza de nueva creación sin necesidad de sujetarse al procedimiento de reclutamiento y selección y sólo pueden ser de nivel mínimo de subdirector de área.
- Perfil de puesto: es el proceso que permite identificar las aptitudes, cualidades y capacidades que, conforme a su descripción, son fundamentales para la ocupación y desempeño del mismo.
- Plantilla de personal: instrumento de información que contiene la relación de los trabajadores que laboran en una unidad administrativa, señalando el puesto que ocupan y el sueldo que perciben.
- Plaza: la posición presupuestaria que respalda un puesto en la estructura ocupacional o plantilla, que sólo puede ser ocupada por un servidor público y que tiene una adscripción determinada.

- Puesto: la unidad impersonal establecida en el Catálogo de Puestos de la Administración Pública Federal Centralizada, que implica deberes específicos y delimita jerarquías y capacidades para su desempeño.
- Puestos adscritos a Áreas de Seguridad Nacional: aquellos puestos pertenecientes a unidades administrativas de la Secretaría de Hacienda y Crédito Público que hayan sido reconocidas como instancias de seguridad nacional.
- Puestos de designación directa: aquellos puestos que no están sujetos a la Ley del Servicio Profesional de Carrera en la Administración Pública Federal, en virtud de que el procedimiento para realizar la designación o expedir el nombramiento de su titular, se encuentra previsto expresamente en alguna disposición a nivel constitucional o legal.
- Puestos de libre designación: los puestos que cumplan con los requisitos señalados en el Articulo 91 del Reglamento de la Ley del Servicio Profesional de Carrera en la Administración Pública Federal, así como con los criterios generales establecidos por la Secretaría de la Función Pública.
- Puestos que no pertenecen al Servicio Profesional de Carrera: aquellos puestos adscritos a la Secretaría de Hacienda y Crédito Público que se encuentran contemplados en el Artículo 8 de la Ley del Servicio Profesional de Carrera en la Administración Pública Federal.
- RLSPCAPF: Reglamento de la Ley del Servicio Profesional de Carrera en la Administración Pública Federal.
- RUSP: Registro Único de Servidores Públicos.
- Servidor público de libre designación: la persona física que desempeña un puesto de libre designación y que no forma parte del Servicio Profesional de Carrera.
- SHCP: Secretaría de Hacienda y Crédito Público.
- SFP: Secretaría de la Función Pública.
- SIARH: Sistema de Información y Administración de Recursos Humanos que opera en forma desconcentrada, con una sola base de datos que permitirá a las coordinaciones administrativas de las unidades de la Secretaria de Hacienda y Crédito Público, tener actualizada permanentemente su plantilla, operar en forma electrónica los movimientos de personal y consultar en línea los reportes que inciden sobre los pagos de nómina.

- Sistema de Video Vigilancia: se refiere al proceso de diseño, implementación, operación y evaluación de los servicios de seguridad prestado a la ciudadanía.
- Unidad de Monitoreo: se refiere al área de funcionamiento y operación de los Sistemas de Video Vigilancia, integrada en un Centro de Control y comando que convive con el CALLE y los procesos de inteligencia policial para contribuir a los objetivos del Sistema Nacional de Seguridad Pública.
- UR o UR's: Unidad Responsable (singular o plural).
- Valuación de Puestos: metodología empleada para determinar el valor en puntos de cada puesto, considerando sus características inherentes, la cual se contiene en el Catálogo Institucional de Puestos.

IV.6.3 Lineamientos normativos.

IV.6.3.1 De los puestos.

El organigrama interno que se sugiere para los Centros contempla los siguientes puestos:

a) Coordinador General del Centro de Control del SVV.
b) Director de Inteligencia y Análisis.
c) Director de Operaciones.
d) Director de Tecnologías de la Información y Comunicaciones.
e) Analista (Inteligencia y Análisis).
f) Coordinador (Operaciones).
g) Supervisor (Operaciones).
h) Operador de Video-Vigilancia.
i) Supervisor de Llamadas de Emergencia.
j) Operador de Llamadas de Emergencia.

IV.6.3.2 De los perfiles.

Cada puesto dentro del organigrama debe cubrir el perfil profesional asociado a cada puesto:

a) Coordinador General del Centro de Control del SVV.
b) Director de Inteligencia y Análisis.
c) Director de Operaciones.
d) Director de Tecnologías de la Información y Comunicaciones.
e) Analista (Inteligencia y Análisis).
f) Coordinador (Operaciones).
g) Supervisor (Operaciones).
h) Operador de Video-Vigilancia.
i) Supervisor de Llamadas de Emergencia.
j) Operador de Llamadas de Emergencia.

IV.6.3.3 De las evaluaciones de control de confianza para los empleados.

Los empleados que laboran para el Sistema de Video-Vigilancia deben presentar y aprobar las evaluaciones de acuerdo a la normatividad estatal y nacional sobre Seguridad Pública en las áreas.

a) Médico toxicológica.
b) Psicológica.
c) Poligráfica.
d) Socioeconómica.

IV.6.3.4 De la medición de la eficacia de los Sistemas de Video Vigilancia.

A la instalación de Sistemas de Video Vigilancia para la seguridad pública, debe continuar el establecimiento de métricas que arrojen evidencia sobre su eficacia.

Con la finalidad de determinar la eficiencia en la utilización de los recursos públicos destinados a su instalación, la operación de los sistemas de Video Vigilancia y sus resultados deben ser monitoreados y medidos con base a parámetros de actuación que permitan observar su impacto en la reducción de los índices delictivos, el aumento de las detenciones y denuncias, o la reducción de los niveles de corrupción.

A continuación se sugieren elementos para establecer métricas de eficacia de los Sistemas de Video Vigilancia, a partir de las mejores prácticas encontradas durante la elaboración de esta Norma Técnica.

En relación a la disminución de los índices delictivos.

Es recomendable establecer una métrica para observar la reducción de robos y otros delitos de orden común, con posterioridad a la implementación del sistema. Esta medición deberá considerar el comportamiento de los índices delictivos en aquellos territorios donde se instaló un Sistema de Video Vigilancia.

En relación al aumento de detenciones.

Se puede medir el número de detenciones derivadas de la utilización de las cámaras la relación, lo que dará un parámetro de la eficiencia policial ligada al uso del sistema de video vigilancia.

En relación al aumento de denuncias.

Se debe establecer una métrica para observar los eventos captados por cámara y los que fueron denunciados. Es decir, cuántos de los eventos captados por las cámaras concluyeron en una denuncia.

En relación a la reducción de los niveles de corrupción.

De igual manera, puede establecerse como indicador la disminución de denuncias por corrupción en la actuación de los cuerpos policiales como resultado de la instalación de Sistemas de Video Vigilancia en determinado territorio.

En relación a los resultados de los servicios de emergencia.

Asimismo, se pueden medir las detenciones relacionadas con el reporte de incidentes al número de emergencias donde hubo participación del Centro de monitoreo.

Es recomendable que la periodicidad de las métricas se establezca por semana, mes y año.